

NASA系统工程手册

NASA Systems Engineering Handbook

朱一凡 李 群 杨 峰 雷永林 侯洪涛 译



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

NASA 系统工程手册

NASA Systems Engineering Handbook

朱一凡 李群 杨峰 雷永林 侯洪涛 译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

系统工程是分析解决复杂系统的论证、设计、生产和使用中的评价决策和权衡优化问题的有效方法和手段。系统工程不仅有完整的理论方法和技术手段构成的科学体系,而且在像航天系统这样经费预算多、研制周期长、运行使用风险高的复杂系统中的具体应用又体现出多样性和复杂性。如何有效地利用系统工程理论和方法针对复杂系统进行组织管理并达到预期的目的,需要对系统工程思想有深刻的理解和丰富的工程实践经验。本手册是美国国家航空航天局(NASA)对多年系统工程实践经验的总结,主要有三个部分的内容:第一部分(第1~3章)是结合航天产品的寿命周期介绍由多个系统工程流程构成的航天产品开发和控制管理的系统工程引擎,第二部分(第4~5章)针对系统工程引擎中的每个流程详细介绍流程实施的过程和指南,第三部分(第6~7章)介绍在开展系统工程工作时应当把握的关键技术和相关标准。

本手册内容翔实、图文并茂,许多问题的阐述结合实例,部分具体操作还在附录中给出了参考样板。NASA系统工程手册不仅可以作为工业工程领域产品开发和系统工程组织管理实践的有益借鉴,也可以作为从事产品研发与项目管理的科技人员和高等院校系统工程专业或相近专业研究生和高年级本科生的学习参考。

本手册部分章节的阅读需参考“NASA项目寿命周期系统工程视图——飞行与地面系统系统工程流程”大图,读者可登录 www.hxedu.com.cn(华信教育资源网)搜索本书免费下载,或发送邮件到 chenwk@phei.com.cn 索取。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

图书在版编目(CIP)数据

NASA 系统工程手册/朱一凡等译. —北京:电子工业出版社,2012.11

ISBN 978-7-121-18081-1

I. ①N… II. ①朱… III. ①航空工程—技术手册②航天工程—技术手册 IV. ①V2-62②V4-62

中国版本图书馆CIP数据核字(2012)第202165号

策划编辑:陈韦凯 特约编辑:刘丽丽

责任编辑:陈韦凯

印 刷:三河市鑫金马印装有限公司

装 订:三河市鑫金马印装有限公司

出版发行:电子工业出版社

北京市海淀区万寿路173信箱 邮编 100036

开 本:787×1092 1/16 印张:21 字数:533千字

印 次:2012年11月第1次印刷

册 数:3000册 定价:65.00元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010)88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010)88258888。

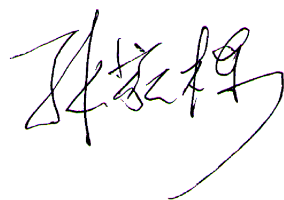
序

我国航天事业经过 50 多年的发展，取得了举世瞩目的成就。在钱学森等老一辈科学家的带领下，我国航天系统工程伴随着中国航天事业的发展而逐步成长、成熟。航天系统工程是运用系统工程的理论和方法对航天工程从需求论证到设计研制、生产制造，以及运行维护等全寿命过程所进行的技术和管理活动的统称，主要关注并解决复杂工程系统总体权衡与优化问题，在“两弹一星”、“载人航天”、“北斗”等大型复杂工程的建设实践中得到充分运用，对保障我国航天工程的顺利实施、增强我国综合实力、带动科技进步、促进经济发展发挥了重大作用。

我国正处于由航天大国向航天强国迈进的关键时期，航天工程的使命任务更加多样化，系统功能越来越复杂，需要进一步探索航天系统工程规律，提升现代宇航能力，积极推动航天事业科学发展。中国卫星导航系统管理办公室一直致力于促进航天系统工程理论和方法在北斗卫星导航系统建设和应用实践中的运用。2012 年底北斗卫星导航系统将完成区域系统建设，提供覆盖亚太地区的导航服务，2020 年将建成全球卫星导航系统。面对前所未有的系统规模、高可靠高质量的应用服务要求、日趋激烈的国际竞争，迫切需要进一步研究航天系统工程理论和方法，有力保障北斗卫星导航系统建设和应用的顺利实施。

在中国卫星导航系统管理办公室的支持下，由国防科技大学系统工程系组织开展了《NASA 系统工程手册》的翻译、出版工作。该书是 NASA 对航天系统工程管理方法、技术和经验的最新概括和总结，反映了 NASA 在航天系统工程领域积累的成功经验。书中介绍的航天系统工程技术和管理方法，对我国航天工程组织实施具有积极的借鉴意义。

中国科学院院士



译者序

自 20 世纪后半叶，在钱学森先生创导下，系统工程如雨后春笋蓬勃发展，在我国的社会发展和经济建设中得到广泛应用并发挥了积极作用。而随着系统工程理论和方法的日渐丰富，以及系统工程技术在社会、经济和军事领域应用的不断深入，对于如何利用系统工程有效解决复杂系统问题，还存在不少认识误区和实践偏差。甚至某些时候复杂的系统工程成为了某些部门回避困难的借口。实际上，在系统的设计研发过程中，系统工程不仅仅是对于系统预测、评价和优化等技术的应用，更多情况下是从宏观上和整体上分析系统，在系统集成设计框架下采用专门技术解决具体问题，寻求系统整体最优的理念和过程。系统工程的实践过程是长期和复杂的，其核心作用在于将所涉及的人员、技术和资源有机地结合在一起，以最有效的方式达到系统目标，而这一点恰恰就是系统工程实践中的困难所在。

美国国家航空航宇局（NASA）曾经组织过多个大型复杂航天系统项目，有着丰富的经验积累和理论沉淀；“阿波罗”载人登月工程和天地往返运输系统（“航天飞机”）就是系统工程应用的成功典范。《NASA 系统工程手册》是对系统工程应用实践经验的总结，该手册结合系统全寿命周期，对系统寿命周期各个阶段对应的系统工程流程，以及各个系统工程流程中的系统工程管理技术进行了详细说明。可以说，这本手册对于系统前期论证和产品设计开发过程中系统工程方法运用和实践具有极高的借鉴和参考价值。

复杂的航天系统各项工程都有各自具体的问题，解决问题的手段和途径也不尽相同，但利用系统工程方法解决系统问题的思路是相通的。《NASA 系统工程手册》一公布，就引起了“北斗”卫星导航专项管理办公室的极大关注。在“北斗”卫星导航专项管理办公室的鼓励和支持下，我们组织力量对《NASA 系统工程手册》进行了翻译，希望这项工作能够对像“北斗”卫星导航工程这样的复杂系统工程项目中的产品设计和项目管理起到辅助作用。由于手册中涉及的学科专业知识广泛、工程历史背景繁杂，翻译中难免有不准确和不精致之处，敬请读者批评指正。

在本手册的翻译过程中，得到了许多同行和专家的指导和帮助，在此表示感谢！感谢“北斗”卫星导航专项管理办公室的领导对本手册的翻译给予的支持和协作；感谢电子工业出版社工业技术出版分社的徐静分社长和陈韦凯编辑为本手册的顺利翻译出版在版权联系和文稿编辑方面付出的努力和给予的指导；感谢王维平教授、郭波教授对于本手册翻译的理解和鼓励，以及总体上的把关和具体事务上的支持。

译者

2012 年 5 月

前 言

自从 1995 年编写 NASA/SP-6105 之后，在美国和国际标准的框架下，作为一门学科，美国国家航空航天局（NASA）的系统工程已经有了迅猛的发展。其主要进步包括实现了国际标准组织的 ISO9000 标准，采用了卡内基梅隆大学软件工程研究所的一体化能力成熟度模型（CMMI）来提升产品的开发和发布，以及减少任务失败的影响。在系统工程方面的经验教训已经写入 NASA 一体化行动小组（NIAT）报告、哥伦比亚号事故调查委员会报告，以及随后的迪亚兹报告。由此产生了 NASA 总工程师办公室（OCE）提高 NASA 系统工程基础和能力的倡议，以获得更有效的 NASA 工程系统，生产更高质量的产品，以实现使命任务的成功。此外，NASA 的系统工程政策和要求已经建立，这本更新后的手册是 OCE 发起的全 NASA 范围的系统工程倡议的一部分。

1995 年 SP-6105 的出版是为了将系统工程的基本概念和技术带给 NASA 的技术人员，以此使他们认识 NASA 系统和 NASA 环境的性质。SP-6105 的修订本保留了这个最初的理念，并更新了 NASA 系统工程知识结构，提供了对了解当前 NASA 最佳实践的指导，并根据新的 NASA 系统工程政策修订了手册。

本手册的更新体现在两个方面：自顶向下兼容 NASA 的高层政策和自底向上汇集 NASA 在本领域从业者的智慧。这种方法建立了科技情报与 NASA 系统工程过程之间的桥梁，便于在 NASA 内部更好地开展系统工程实践。本手册试图说明良好实践及方案的原则，而不是强调完成某个使命任务的特定方法。本手册集成的是 NASA 系统工程实践独特的顶层实现方法。本手册的更新过程中采用的材料有多种来源，包括 NASA 工程上的要求、外场系统工程手册和流程，以及非 NASA 的系统工程教材和指导书。

本手册包括 6 个核心章节：（1）系统工程基础讨论；（2）NASA 工程/项目寿命周期；（3）从概念到设计的系统工程流程；（4）从设计到最终产品的系统工程流程；（5）系统工程流程的交互关联技术管理；（6）与系统工程相关的特别专题。用于充实这些核心章节的附录提供各章主题的要点、案例及其他附加信息。本手册还使用注记和图形用于核心章节中的概念定义、理论深化、具体说明和概念拓展，而不会使读者的兴趣偏离各章节中的主要内容。

本手册为良好的系统工程实践提供自顶向下的指导，而不是以任何方式提出指令。

NASA/SP-2007-6105 修订版就此取代 1995 年 6 月颁布的 SP-6105。

目 录

第 1 章	引言	1
1.1	本手册的目的	1
1.2	本手册的范围和深度	1
1.3	关于 NASA	1
第 2 章	系统工程基础	4
2.1	通用技术流程与系统工程引擎	5
2.2	按照项目阶段概述系统工程引擎	6
2.3	使用系统工程引擎的示例	7
2.3.1	示例导言	9
2.3.2	详细示例	9
2.4	产品验证和产品确认的区别	16
2.5	系统工程的费用	16
第 3 章	NASA 工程/项目寿命周期	19
3.1	工程规划论证	20
3.2	工程实施执行	21
3.3	项目 A 前阶段：概念探索	22
3.4	项目阶段 A：概念研究和技术开发	23
3.5	项目阶段 B：初步设计和技术完善	24
3.6	项目阶段 C：详细设计和制造	25
3.7	项目阶段 D：系统组装、集成、试验和投产	27
3.8	项目阶段 E：运行使用与维护	28
3.9	项目阶段 F：退役处置	28
3.10	经费：预算周期	29
第 4 章	系统设计	31
4.1	明确利益相关者的期望	32
4.1.1	流程描述	32
4.1.2	明确利益相关者期望流程指南	35
4.2	技术需求定义	39
4.2.1	流程描述	39
4.2.2	技术需求定义指南	41
4.3	逻辑分解	48
4.3.1	流程描述	48

4.3.2	逻辑分解指南·····	51
4.4	设计方案定义·····	54
4.4.1	流程描述·····	54
4.4.2	设计方案定义指南·····	61
第 5 章	产品实现·····	69
5.1	产品实施执行·····	69
5.1.1	流程描述·····	70
5.1.2	产品实施执行指南·····	73
5.2	产品集成·····	74
5.2.1	流程描述·····	75
5.2.2	产品集成指南·····	77
5.3	产品验证·····	80
5.3.1	流程描述·····	80
5.3.2	产品验证指南·····	86
5.4	产品确认·····	94
5.4.1	流程描述·····	95
5.4.2	产品确认指南·····	101
5.5	产品交付·····	102
5.5.1	流程描述·····	102
5.5.2	产品交付指南·····	106
第 6 章	技术管理·····	108
6.1	技术规划·····	108
6.1.1	流程描述·····	109
6.1.2	技术规划指南·····	120
6.2	需求管理·····	129
6.2.1	流程描述·····	129
6.2.2	需求管理指南·····	133
6.3	接口管理·····	134
6.3.1	流程描述·····	134
6.3.2	接口管理指南·····	135
6.4	技术风险管理·····	136
6.4.1	流程描述·····	137
6.4.2	技术风险管理指南·····	139
6.5	技术状态管理·····	149
6.5.1	流程描述·····	149
6.5.2	技术状态管理指南·····	155
6.6	技术数据管理·····	156
6.6.1	流程描述·····	157

6.6.2	技术数据管理指南	163
6.7	技术评估	164
6.7.1	流程描述	164
6.7.2	技术评估指南	166
6.8	决策分析	193
6.8.1	流程描述	194
6.8.2	决策分析指南	199
第 7 章	相关专题	212
7.1	与合同相关的工程技术	212
7.1.1	引言、目的和范围	212
7.1.2	采办策略	212
7.1.3	签订合同前的工作	216
7.1.4	履行合同期间	222
7.1.5	合同完成	224
7.2	一体化设计平台	227
7.2.1	引言	227
7.2.2	CACE 概述及其重要性	228
7.2.3	CACE 目标和益处	228
7.2.4	CACE 人员组织	229
7.2.5	CACE 流程	229
7.2.6	CACE 工程的工具和技巧	231
7.2.7	CACE 设施、信息架构和人员组织	231
7.2.8	CACE 产品	232
7.2.9	CACE 最佳实践	233
7.3	选择工程设计工具	234
7.3.1	工程和项目考虑的事项	234
7.3.2	政策和流程	235
7.3.3	协同	235
7.3.4	设计标准	235
7.3.5	现有的信息体系结构	236
7.3.6	工具接口	236
7.3.7	互操作性和数据格式	236
7.3.8	向后兼容性	236
7.3.9	平台	237
7.3.10	工具技术状态控制	237
7.3.11	保密性/访问控制	237
7.3.12	培训	237
7.3.13	许可证	237
7.3.14	供应商和用户保障的稳定性	238

7.4 人因工程	238
7.4.1 基础人因模型	239
7.4.2 人因分析和评估技术	240
7.5 环境、核安全、行星保护和资产保护政策约束	245
7.5.1 美国国家环境政策法令和行政法令	245
7.5.2 关于放射性物质的环境影响	247
7.5.3 行星保护	248
7.5.4 空间资产设施保护	249
7.6 公制度量单位的使用	250
附录 A 缩略词	253
附录 B 专用词汇表	258
附录 C 如何撰写一个好的需求	271
附录 D 需求验证矩阵	274
附录 E 创建确认计划（包括需求确认矩阵）	275
附录 F 功能、时序和状态分析	276
附录 G 技术评估/技术引入	283
附录 H 集成计划概要	290
附录 I 验证和确认范例概要	292
附录 J 系统工程管理计划内容概要	294
附录 K 计划	299
附录 L 接口需求文档概要	301
附录 M 技术状态管理（CM）计划概要	303
附录 N 技术同行评审/检查	304
附录 O 权衡示例	308
附录 P 任务书（SOW）评审清单	309
附录 Q 项目防护规划概要	312
分章节参考文献	314
按作者参考文献	319

第 1 章 引言

1.1 本手册的目的

本手册意图在系统工程方面为 NASA（美国国家航空航天局）全体人员提供有用的总体指导和相关信息。它提供系统工程应用于 NASA 时的一般描述。本手册的目的是提升全 NASA 对系统工程认知的一致性，并促进系统工程实践。本手册提供与 NASA 相关的观点和特定用于 NASA 的数据。

本手册应当与 NPR 7123.1《系统工程流程和需求》及 NASA 中心制定的在 NASA 内实行系统工程的手册和指令共同使用。

1.2 本手册的范围和深度

本手册的覆盖范围限于流程、工具和技巧的一般概念和描述。它提供系统工程最佳实践的信息和需要避免的易犯错误。更深入的学习可参考 NASA 中心制定的专用手册和指令，以及相关的教科书。

本手册应用于大型或小型 NASA 工程和项目的开发和实施过程中的系统工程。NASA 针对主要的项目类别和产品系列定义了不同的寿命周期，如飞行系统和地面保障，理论研究与技术开发，试验基地建设，环境合规与恢复。本手册提供的系统工程最佳实践的技术内容应当成为 NASA 所有产品系列的组成部分（请查询 NASA 在线指导信息系统 NODIS 电子文档数据库，获取与产品系列等相关的 NASA 指导）。为了简便，本手册使用飞行系统和地面保障作为相关产品的例子。飞行系统和地面保障的具体内容可以参见其寿命周期描述和里程碑评审的详细内容。在这两个领域中产品系列是不同的，因此，读者应当参考 NASA 技术规程需求的适当部分来获取其寿命周期和评审的特殊要求。NASA 的系统工程是一个有条不紊的过程，该过程在 NASA 计划和项目的全寿命周期中循环反复地用于系统的设计、研发、运行、维护和退役阶段。

本手册适当地覆盖了系统工程的功能范围，不管它是由管理人员负责还是由工程师负责，也不管它是在 NASA 内部实施，还是由承包商实施。

1.3 关于 NASA

关于 NASA 的情况介绍如下：

(1) NASA 总部（NASA Headquarters）位于美国华盛顿哥伦比亚特区，NASA 的组织结构及 NASA 总部的作用如图 1.3-1 所示。

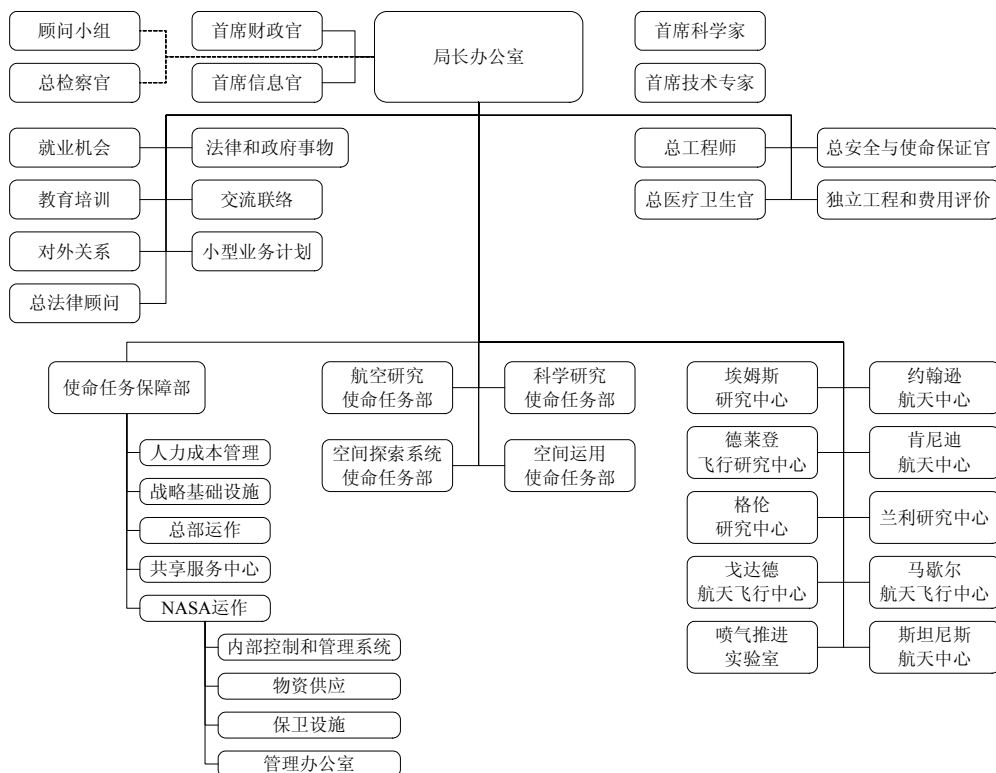


图 1.3-1 NASA 组织结构及 NASA 总部的作用

(2) NASA 埃姆斯研究中心 (NASA Ames Research Center) 位于美国加利福尼亚州硅谷的莫菲特军事管理区。该中心的主要研究对象集中在信息技术领域，包括超级计算、计算机网络和智能系统等。约瑟夫·埃姆斯 (Joseph S. Ames, 1864—1943) 是美国国家航空咨询委员会 (National Advisory Committee for Aeronautics, NACA, NASA 的前身) 的缔造者之一，于 1919—1939 年长期担任 NACA 的主席。

(3) NASA 德莱登飞行研究中心 (NASA Dryden Flight Research Center) 位于美国加利福尼亚州爱德华兹空军基地，是美国航天飞机运输机的大本营，负责将返回着陆后的航天飞机用改装的波音 747 飞机运回肯尼迪航天中心。休·德莱登 (Hugh L. Dryden, 1898—1965) 是美国杰出的航空航天系统工程师，1947—1958 年任 NACA 主席，1958 年起 NACA 编入 NASA 之后任 NASA 副局长。

(4) NASA 格伦研究中心 (NASA Glenn Research Center) 位于美国俄亥俄州克利夫兰市，该中心的主要研究对象集中在空间飞行系统，重点是空气推进、空间推进、动力系统及核能装置。约翰·格伦 (John Glenn, 1921—) 是美国第一位进入太空飞行的宇航员。1962 年 2 月 20 日，约翰·格伦乘坐的“友谊七号”宇宙飞船由美国水星-6 火箭发射升空。

(5) NASA 戈达德航天飞行中心 (NASA Goddard Space Flight Center) 是 NASA 最重要的空间研究实验室之一，位于美国马里兰州格林贝尔特镇，主要负责无人空间飞行器的开发与运用，以及获取太阳系和宇宙的观测数据及知识。罗伯特·戈达德 (Robert H. Goddard, 1882—1945) 是美国火箭工程学的先驱者，液体火箭的发明人。1926 年 3 月 16 日在马萨诸塞州奥本成功发射了世界上第一枚液体火箭。

(6) 喷气推进实验室 (Jet Propulsion Laboratory) 位于美国加利福尼亚州的帕萨迪纳, 是美国无人飞行器探索太阳系的研究中心, 负责为 NASA 开发和管理无人空间探测任务。

(7) NASA 约翰逊航天中心 (NASA Johnson Space Center) 位于美国德克萨斯州休斯顿市克里尔湖畔, 1964 年建成运转。1973 年为纪念当年去世的前总统林登·约翰逊改用现名。该中心主要负责设计、研制和试验载人飞船系统, 选拔和训练航天员, 以及计划和实施载人飞行任务。林登·约翰逊 (Lyndon B. Johnson, 1908—1973) 是美国第 36 任总统 (1963—1969), 因其在任期间所制定的外交政策, 致使越战不断升级, 美军伤亡惨重。

(8) NASA 肯尼迪航天中心 (NASA Kennedy Space Center) 位于美国佛罗里达州东海岸的梅里特岛卡纳维拉尔角, 是 NASA 进行载人/无人航天器测试、准备和实施发射的最重要的场所。约翰·肯尼迪 (John Kennedy, 1917—1963) 是美国第 35 任总统 (1961—1963), 曾以强硬态度处理古巴导弹危机, 1963 年 11 月在美国德克萨斯州的达拉斯遇刺身亡。

(9) NASA 兰利研究中心 (Langley Research Center) 位于美国弗吉尼亚州的汉普顿, 是 NASA 成立时最早的研究机构之一, 目前是 NASA 结构与材料领域的重点研究中心, 负责研发和测试新型材料和新结构。

(10) NASA 马歇尔航天飞行中心 (NASA Marshall Space Flight Center) 位于美国阿拉巴马州的亨茨维尔, 是 NASA 的原根据地, 是负责航天飞机推进、空间飞行器推进、人员训练、有效载荷、国际空间站及信息管理的中心。乔治·马歇尔 (George Marshall, 1880—1959) 是美国的军事家、政治家和外交家, 陆军五星上将, 1947—1949 年任美国国务卿, 1950—1951 年任美国国防部长, 1953 年获诺贝尔和平奖。

(11) NASA 斯坦尼斯航天中心 (NASA Stennis Space Center) 位于美国密西西比州汉考克 (Hancock) 县, 是 NASA 的火箭推进试验基地。约翰·斯坦尼斯 (John Stennis, 1901—1995) 是来自密西西比州的美国最著名的参议员, 因推动美国海军大型改造计划获得“美国现代海军之父”的美称。以其名字命名的“斯坦尼斯”号核动力航空母舰于 1993 年 11 月正式下水, 1995 年 6 月加入现役。

第2章 系统工程基础

系统工程是用于系统设计、实现、技术管理、运行使用和退役的专业学科方法论。系统由不同的元素组成，这些元素相互作用产生单个元素无法产生的效果。系统元素或组成部分包括人员、硬件、软件、设施、政策和文档等为产生系统级结果所需的事物。这些结果包括系统级品质、属性、特征、功能、行为和性能。系统作为整体所产生的价值来自于各组成部分的相互联系和相互作用关系，又远远超过各组成部分的独立贡献。系统工程是技术决策时查看系统“全貌”的途径，是在确定的使用环境下和规划的系统生命周期中达到利益相关者性能需求的途径。换句话说，系统工程是一种逻辑思维的方法。

系统工程是在通常有相反作用的约束下，开发满足系统需求可行系统的科学和艺术。系统工程是一门综合的、整体的学科，通过相互比较来评价和权衡结构设计师、电子工程师、机械工程师、电力工程师、人因工程师，以及其他学科人员的贡献，形成一致的不被单一学科观点左右的系统整体。

系统工程方法面对不同利益和多样化甚至冲突的约束，寻找安全平衡的设计方案。系统工程师必须提高技能，确定并关注优化系统整体而非单一子系统设计的评估工作。了解何时何地探索是一门艺术。有此技能的人员通常称为“系统工程师”，或其他头衔如首席工程师、技术负责人、主任工程师等，本手册使用系统工程师这个术语。

依据项目的规模和复杂度及寿命周期的阶段划分，系统工程师的具体作用和职责随项目不同而发生变化。针对大型项目，可能需要一个或多个系统工程师，而针对小型项目，有时则由项目负责人担任此项工作。但是，无论安排谁承担这些职责，系统工程师的功能必须履行。系统工程师的实际作用和职责是按其头衔变化的。首席系统工程师确保系统开发遵循合适的系统工程方法，系统在技术上能够完成规定的需求。系统工程师监督技术团队开展系统工程活动，对任务进行指导、交流、监督和协调。系统工程师审查和评价项目的技术状况，确保系统/子系统的系统流程正常发挥作用，推进系统从概念到产品的演化。技术团队应整体介入到系统工程流程中。

系统工程师在引导系统架构的开发、需求的定义和分配、设计方案的评价与权衡、系统间技术风险均衡、系统接口的定义和评估、验证和确认活动的全面监督，以及许多其他任务中起关键的作用。通常系统工程师的另一个主要任务是开发项目文档，包括系统工程管理计划、需求/规范文档、验证和确认文档、证明材料及其他技术文档。

总的来说，系统工程师擅长平衡复杂系统在组织和技术方面的相互作用。既然整个团队参与系统工程过程，某种意义上说每个成员都是系统工程师。系统工程关注于折中和权衡，需要的是总体人员而不是专业人员。系统工程观察“系统全貌”，不仅确保设计正确的系统（满足需求），还要确保正确的系统设计。

为进一步探讨，将系统工程放在项目管理的背景下。依据 NPR 7120.5《NASA 空间飞行工程和项目管理需求》，项目管理是在一定的费用、品质及进度约束下，为达到客户和其他利益相关者的需求、目的和目标所要进行的大量活动的规划、监督和指导。项目管理有两个同

样重要的研究领域，即系统工程和项目控制。图 2.0-1 给出这两个领域的关系，可以看出项目管理的这两个研究领域具有重叠的部分。系统工程为重叠部分提供技术层面的输入，而项目控制主要提供规划、费用及进度方面的输入。

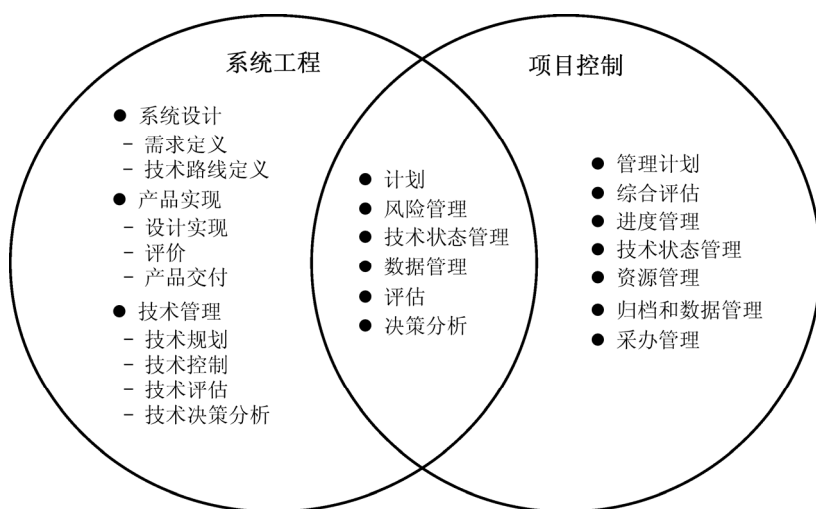


图 2.0-1 系统工程在全面项目管理背景中的总体描述

本手册关注的是图 2.0-1 中的系统工程部分，其中的实践/流程来源于 NPR 7123.1《NASA 系统工程流程和需求》。本书后续各章将对每个流程作详细介绍，本章只作总体介绍。

2.1 通用技术流程与系统工程引擎

在 NPR 7123.1《NASA 系统工程流程和需求》中包括三类技术流程：系统设计、产品实现及技术管理。三类技术流程及相互间交互和数据流关系如图 2.1-1 所示。系统工程引擎用于目标产品的开发和实现。本章介绍 NPR 7123.1 需要的 17 个通用技术流程的背景知识。系统设计流程、产品实现流程，以及技术管理流程将分别在第 4 章、第 5 章和第 6 章中作详细介绍。图 2.1-1 所示的步骤 1~步骤 9 描述实施一个项目时的任务，步骤 10~步骤 17 是执行这些流程的关联工具。

系统设计流程：图 2.1-1 给出 3 个系统设计流程，主要用于定义利益相关者期望并确定控制基线、生成技术需求并确定控制基线、将技术需求转变为设计方案使之满足控制基线确定的利益相关者期望。这些流程应用于系统结构中每个分支上的产品；系统结构自顶向下分解到可制造、购买或重用的底层产品。系统结构中的其他产品通过底层产品的集成而获得。设计师不仅开发完成系统特定功能的产品设计方案，还需建立产品和服务需求以保证能够获得系统结构中的所有运行使用产品/使命任务产品。

产品实现流程：产品实现流程应用于系统结构中每一个运行使用产品/使命任务产品，自最底层产品到高层的集成产品。这些流程用于生成每个产品的设计方案（如产品实施执行或产品集成），同时用于验证和确认产品，并将相应产品作为寿命周期阶段的一项功能产品交付到更高的产品层次中，从而满足该层次设计方案，同时满足利益相关者的期望。

技术管理流程：技术管理流程用于建立和变更项目的技术规划，管理系统跨界面的交流，

根据计划和需求对系统产品和服务的进展进行评估，控制项目的技术实施，以及辅助决策过程直到项目的完成。

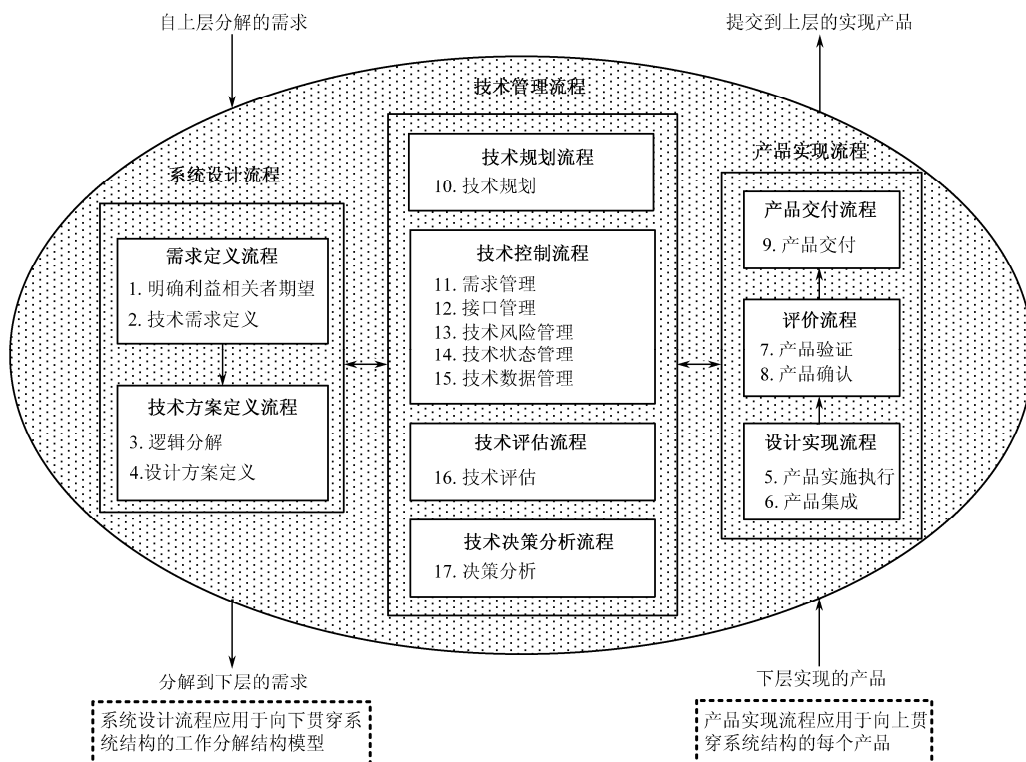


图 2.1-1 系统工程引擎

系统工程引擎中的流程以迭代递归的方式应用。根据 NPR 7123.1 定义，“迭代”是指“应用于同一个（系列）产品，纠正发现的差异或其他需求偏差的过程”，而“递归”是指“流程反复应用于系统结构中较低层次产品的设计或较高层次目标产品的实现”以增加系统的价值。“递归也可以反复应用于寿命周期下一阶段中系统结构的同一流程，以完善系统定义并满足阶段成功准则。”在 2.3 节中给出的示例将进一步解释上述概念。在将系统初始概念分解到足够具体层次的过程中，通用技术流程反复迭代应用，技术团队据此信息可研制产品。随后通用技术流程反复迭代应用于将最小的产品集成到更大的产品中，直到完成系统整体组装、验证、确认和交付。

2.2 按照项目阶段概述系统工程引擎

图 2.2-1 给出项目的 7 个阶段及各阶段如何使用系统工程引擎的概念描述。图 2.2-1 所示的是一个概念框图，详细的流程图可登录 www.hxedu.com.cn（华信教育资源网）搜索本书免费下载，或发送邮件到 chenwk@phei.com.cn 索取。

图中最顶层部分描述项目的系统成熟度，反映从可行概念到系统部署的项目进展过程、各阶段的活动、关键决策点及主要的项目评审。

图中中间部分描述每个项目阶段的技术开发流程（步骤 1～步骤 9）。系统工程引擎从 A 阶段到阶段 D 循环 5 次。需要注意的是，阶段 C 和阶段 D 反映 NASA 管理层将一个技术开发流程分成两部分，这样确保更紧密的管理控制。阶段 C 和阶段 D 的系统工程引擎由短划线框标出。

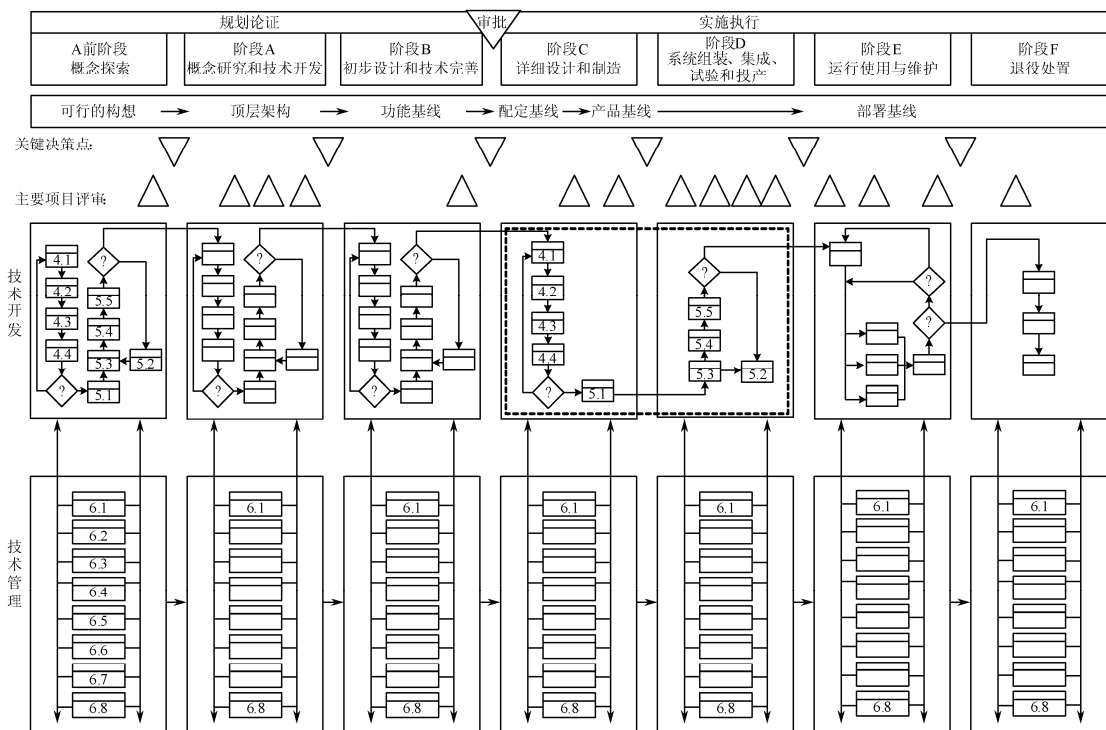


图 2.2-1 本手册中 NASA 飞行和地面系统项目示例寿命周期流程简化概念图

项目一旦进入运行使用阶段（阶段 E）并在退役处置阶段（阶段 F）终止，技术工作也就相应地转移到这最后两个项目阶段的活动中。

图中下半部分描述每个项目阶段的 8 个技术管理流程（步骤 10～步骤 17）。系统工程引擎从 A 前阶段到阶段 F 将技术管理流程循环 7 次。

图中系统工程引擎的每个模块上有一个段落标识，分别对应本手册第 4 章、第 5 章、第 6 章中的各节。例如，技术开发流程中“获取利益相关者期望”将在 4.1 节详细讨论。

2.3 使用系统工程引擎的示例

为了帮助了解系统工程引擎是如何应用的，这里提供一个实例并运行整个流程。相关讨论围绕工程和项目的寿命周期展开，第 3 章将有更深入的讨论。正如第 3 章所描述的那样，NPR7120.5 为 NASA 工程和项目定义了寿命周期概念。寿命周期的阶段划分见表 2.3-1。

表 2.3-1 项目寿命周期的阶段

阶 段		目 的	典 型 输 出
规划论证阶段	A 前阶段	广泛收集关于使命任务的建议和方案，从中选择新的工程和项目。确定所期望系统的可行性，开发使命任务概念，草拟系统级需求，辨识潜在技术要求	以仿真、分析、研究报告、模型和样机形式表示的可行系统概念
	概念探索		

续表

阶 段		目 的	典 型 输 出
规划论证阶段	阶段 A 概念研究和技术开发	确定新的重大系统建议的可行性和迫切性，并建立 NASA 战略计划的初始控制基线兼容性。开发最终使命任务构想、系统级需求和确定需要开发的系统结构技术	以仿真、分析、工程模型和样机形式表示的系统概念，给出权衡研究定义
	阶段 B 初步设计和技术完善	足够详细地定义项目，建立能够达到使命任务需求的初始控制基线。提出系统结构目标产品（及辅助产品）的需求，生成每个系统结构目标产品的初步设计	以样机、权衡研究结果、规范和接口文档，以及原型形式表现的目标产品
实施执行阶段	阶段 C 详细设计和制造	完成系统（及其关联子系统，包括运行系统）的详细设计，进行硬件制造和软件编码。生成每个系统结构目标产品的详细设计	目标产品详细设计、目标产品组件制造和软件开发
	阶段 D 系统组装、集成、试验和投产	将产品组装和集成为系统，同时确信其能够满足系统需求。投入生产并准备运行使用。实施系统目标产品的研制、组装、集成和试验，并交付使用	在相关辅助产品支持下的可运行使用的系统目标产品
	阶段 E 运行使用与维护	执行系统使命任务，实现最初确定的需求并且维持对需求的保障。执行使命任务的运行使用计划	所期望的系统
	阶段 F 退役处置	执行阶段 E 中制定的系统退役/处置计划，对反馈的数据和样本进行分析	产品终止使用

进行寿命周期的阶段划分，可以描述项目的不同产品从初始概念，到产品成型，再到最终退役的逐渐发展和成熟的过程。图 2.1-1 中所示的是系统工程引擎覆盖寿命周期所有的阶段。

在 A 前阶段，系统工程引擎用于开发初始概念；制定初步/概要的关键顶层需求集；通过模型、样机、仿真或其他手段实现这些概念；验证和确认这些概念和产品将能够满足关键顶层需求。注意：这不是在最终产品上执行的正式验证和确认程序，而是方法上的普查，确保在 A 前阶段提出的概念能满足利益相关者可能的要求和期望。概念开发应向下直达所需要的最底层，以确保概念是可行的并将风险降低到满足项目要求的水平。理论上，该流程可以推进到每个系统的元器件层次。但是，这将消耗大量的时间和费用。也许只要达到某个比元器件更高的层次，就能使设计人员准确地确定完成项目的可行性（A 前阶段的目的）。

在阶段 A，系统工程引擎继续递归应用，在此应用中提取 A 前阶段开发和确认的概念和初步关键需求，将其充实为系统需求和运行使用构想（Conops）的控制基线集。在这一阶段，应当对高风险的关键领域建模仿真和建立原型，确保开发的设计和需求的良性的，并确定在随后阶段将使用验证和确认工具及技术。

在阶段 B，系统工程引擎仍被递归应用，来进一步完善待开发产品树中所有产品的需求，开发运行使用构想的初步设计，并进行验证和确认方案的可行性分析，以确保设计尽可能地满足系统需求。

阶段 C 再次使用系统工程引擎的系统设计流程，最终更新确定所有的需求，确定运行使用构想，开发产品结构树最底层产品的详细设计并开始制造。

阶段 D 使用系统工程引擎的产品实现流程，递归实施目标产品的详细研制、集成、验证和确认，并将目标产品交付给用户。

在阶段 E 和阶段 F 使用系统工程引擎的技术管理流程监测绩效、控制技术状态，进行系统运行、维护工程和退役处置的相关决策。现有系统的任何新增能力或升级都将作为新项目重新使用系统工程引擎来进行开发。

2.3.1 示例导言

这里采用众所周知的 NASA 的空间运输系统 (STS) 作为例子来展示如何在阶段 A 使用系统工程引擎。这个例子将简要说明在系统工程引擎中系统工程流程的应用,而不是详细到足以实际建造高度复杂的飞行器。通过递归应用系统工程引擎,在每个步骤获取越来越多的细节。图 2.3-1 中的图标用来标示系统工程引擎的使用位置。图中的序号与图 2.1-1 中所示的系统工程引擎中的流程标号相符。产品分成多个层次。基本上,层次的编号越大,产品在产品分层中的层级就越低并且产品信息也变得更详细(如从机箱细化到电路板,再细化到元器件)。

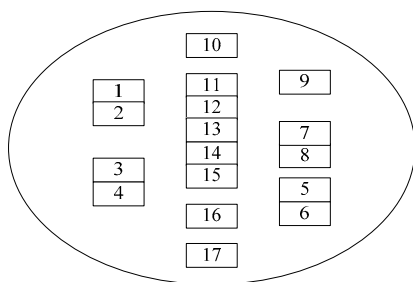


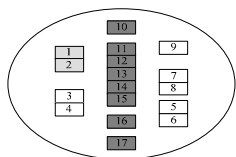
图 2.3-1 系统工程引擎流程图标

2.3.2 详细示例

NASA 确认需要一个运输系统,负责像“卡车”一样将大量的设备部件和人员运送到近地球轨道。参考前述项目寿命周期划分,该项目首先进入 A 前阶段。在这个阶段,进行若干概念研究,并确定开发这种“空间卡车”是可行的。这是结合仿真、样机、分析及其他手段研究之后确定的。为简单起见,假设可行性能通过概念模型得以证明。系统工程引擎的流程和框架用于设计和实现这些模型。随后该项目进入阶段 A 的活动,完善 A 前阶段的概念方案并且定义目标产品的系统需求。详细示例从阶段 A 开始并且显示系统工程引擎如何使用。正像概述中描述的,类似的流程也应用于项目其他阶段。

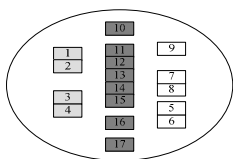
2.3.2.1 阶段 A 示例: 系统设计步骤

1. 第一步



考虑 A 前阶段开发的初步概念方案和关键系统需求,系统工程引擎进入第一个流程,用来确定谁是产品(即 STS)的利益相关者及他们想要什么。在 A 前阶段这些需求和期望是总体的想法,也许只是说 NASA 需要一个“空间卡车”,携带若干吨有效载荷进入近地球轨道,容纳某尺寸的有效载荷,携带 7 名乘员等。在阶段 A 的这一步,这些普通概念将细化并获得一致同意。该阶段生成的运行使用构想同样将细化并获得一致同意,确保所有的利益相关者对产品(这里指运输系统)的真实期望取得一致意见。细化的期望转化为良好的需求陈述(关于如何构成良好陈述的需求,更多信息参见附录 C)。后续的步骤和阶段将需求改进成可实际操作规范。还应注意到,技术管理流程(系统工程引擎中编号 10~17 的流

程)同样在该步骤及后续步骤和活动中应用,确保所有使用和维护的计划、控制、评估和决策是适当的。尽管为了简化本例而不再提及这些流程,但它们的影响总是存在的。



随后,使用前期开发的需求和运行使用构想建立逻辑分解模型/图表,将需求转变为视图并显示它们的关系。最终,这些图表、需求和运行使用构想文件被用来开发一个或多个可行的设计解决方案。注意:既然这只是系统工程引擎全程的第一阶段,这些设计解决方案对于任何实际建立的系统来说都不够详细。因此,设计方案可归纳为“为实现这个运输系统,经过权衡研究,最佳选择是由三个部分组成的系统:运载乘员和货物的可重用轨道器、大型外部燃料箱和为发射提供额外动力的返回式可翻新重用的两个固体火箭助推器。”(当然,实际的设计方案会有更详细的描述)。所以,对于第一步,产品第一层可能看起来类似图 2.3-2。其他辅助产品也可能出现在产品结构树中,但为了简化本例仅展示主要产品。

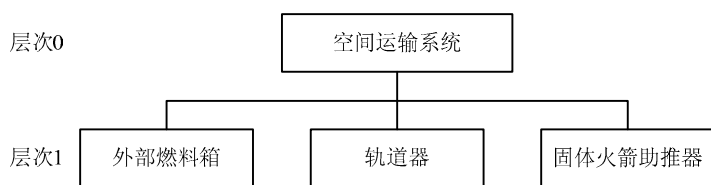
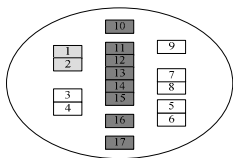


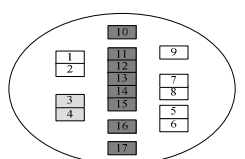
图 2.3-2 产品层次划分,第1层:系统工程引擎第一步

很明显,设计解决方案还未详细到足以建立这些产品的原型或模型的水平。这些需求、运行使用构想、功能图和设计解决方案仍处于相当高的概要层次。注意:系统工程引擎右侧的系统工程流程(即产品实现流程)还需要说明。在应用系统工程引擎右侧流程之前,首先设计必须保证系统在可实际建造、编码或重用的水平上。由此开始执行系统工程引擎左侧流程的第二步。

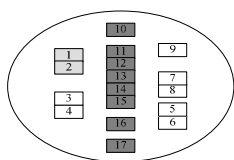
2. 第二步



系统工程引擎是完全递归的。即在第1层图中的三个组件都可以认为自身是一个独立产品,而系统工程引擎可应用到其中任何一个。例如,将外部燃料箱看做一个目标产品并重启系统工程引擎第一个流程。现在只需针对外部燃料箱,确定利益相关者和他们对外部燃料箱的期望。当然,主要利益相关者之一是第1层需求和目标产品 STS 的拥有者,但也有其他新的利益相关者。如此生成新的关于外部燃料箱如何运用的运行使用构想。第1层应用到(分配给)外部燃料箱的需求将“向下分解”并得到确认。通常,其中一些需求过于笼统而不能设计实现,必须进行细化。对于这些派生需求,还将出现来自于利益相关者期望的附加需求,以及技能、安全、质量等方面的应用标准。



随后,与 STS 产品第一步相同,建立外部燃料箱的需求和运行使用构想,并生成功能开发的图表。最终,这些图表、要求和运行使用构想文件被用于开发外部燃料箱的可行设计方案。在这一步,同样没有足够的细节来真正建造或建立外部燃料箱原型。该设计方案可以概括为“为建造此外部燃料箱,权衡研究显示最好的选择是使用低温推进剂,需要用于盛放液氢和液氧的两个燃料箱,以及相关仪器设备和覆盖泡沫材料的铝制外部结构。”这样,外部燃料箱的第2层产品树可能如图 2.3-3 所示。



以类似的方式，轨道器也将通过系统工程引擎执行第二步，确定利益相关者和他们的期望，并为轨道器生成运行使用构想。适合轨道器的第一层需求将被“向下分解”和确认；由此派生的新需求和附加要求（包括与其他组件的接口）将被添加。

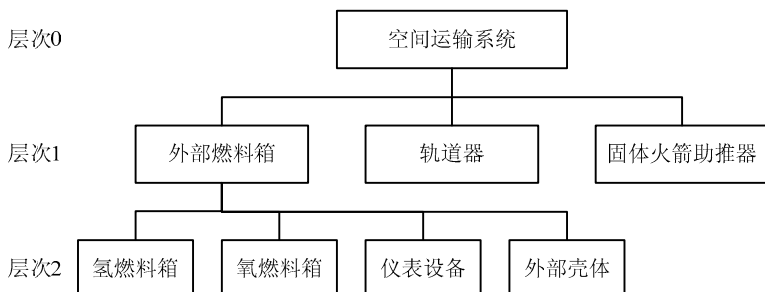
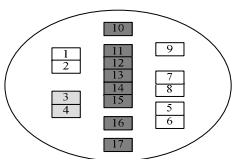


图 2.3-3 产品层次划分，第2层：外部燃料箱



随后，根据轨道器的需求和运行使用构想开发功能图表，生成一个或多个的轨道器设计方案。与外部燃料箱一样，在这一步中不会有足够的细节真正建造轨道器或建立轨道器复杂模型。轨道器设计方案可归纳为“为建立此轨道器将需要一个有翼飞行器，配备热防护系统、飞航电子系统、指挥/导航和控制系统、推进系统和环境控制系统等。”因此，

轨道器组件的第2层产品树可能如图 2.3-4 所示。

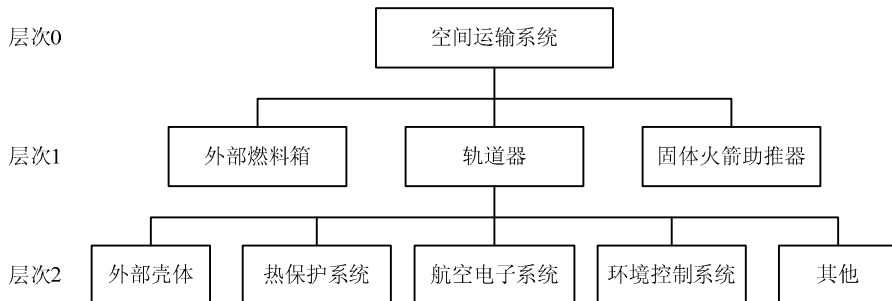
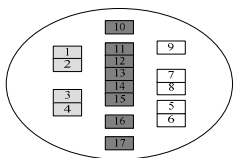


图 2.3-4 产品层次划分，第2层：轨道器

同样，固体火箭助推器也可以看做是目标产品，并像对于外部燃料箱与轨道器所做的那样通过系统工程引擎产生一个第2层的设计方案。

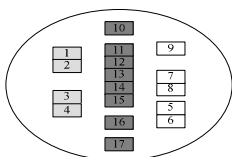
3. 第三步



第2层的每个组件也可被认为是目标产品，并且通过系统工程引擎执行下一步，确定利益相关者，产生运行使用构想，也可以向下分配需求，产生新的和派生的需求，开发功能图表和设计解决方案。以飞航电子系统为例，第3级产品树可能如图 2.3-5 所示。

4. 第四步直到第 n 步

递归过程对各层上每个产品（模型）持续进行，直到产品树的最底层，形成阶段 A 的所有步骤。注意：某些项目中，当给定成本和进度限制时，在阶段 A 中递归流程执行到最小组



件可能并不现实。在这种情况下，必须根据工程技术经验判断可行的产品层次。注意：根据产品的复杂性，可行的最低层次可能有所不同。例如，对于某个产品可能会递归到第 2 层，而对于更复杂的产品，可能递归到第 8 层。这也意味着达到最底层需要不同的时间。因此，对于确定的工程或项目，产品可能需要在不同层级开发。对于本例的阶段 A，图 2.3-6 给出完全通过系统工程引擎的系统设计流程 STS 产品的层次图。完成这些步骤后，产生产品树中每个产品的系统需求、运行使用构想及顶层的功能和物理概念结构。注意：这些只是对目标产品的初步设计，尚没有细化。细化需要在系统寿命周期后期完成。至此，足够的概念设计工作已经完成，至少确保能够达到后续步骤中明确的高风险需求。

阶段 A，图 2.3-6 给出完全通过系统工程引擎的系统设计流程 STS 产品的层次图。完成这些步骤后，产生产品树中每个产品的系统需求、运行使用构想及顶层的功能和物理概念结构。注意：这些只是对目标产品的初步设计，尚没有细化。细化需要在系统寿命周期后期完成。至此，足够的概念设计工作已经完成，至少确保能够达到后续步骤中明确的高风险需求。

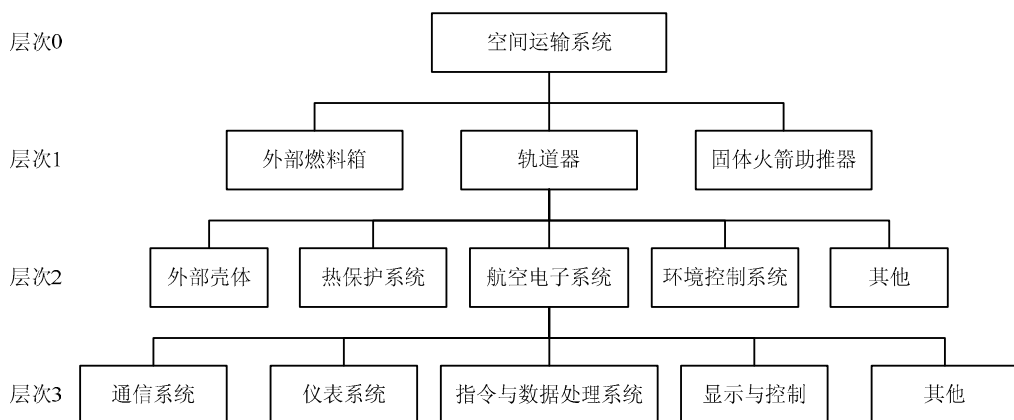


图 2.3-5 产品层次划分，第 3 层：飞航电子系统

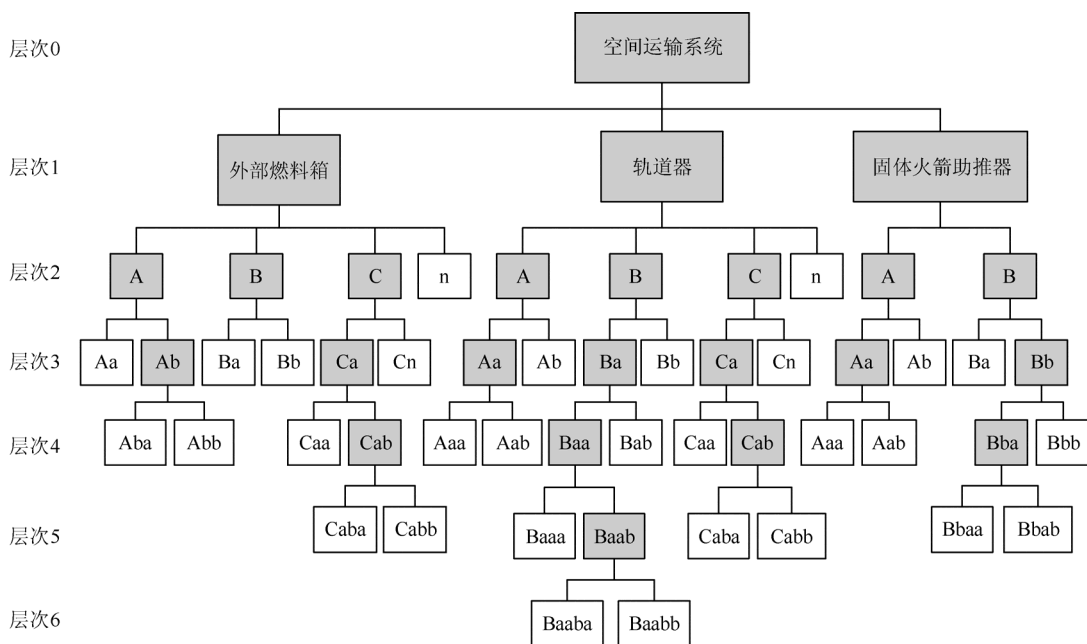


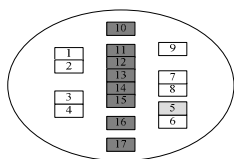
图 2.3-6 产品层次划分：系统工程引擎左侧系统设计流程的完整步骤

2.3.2.2 产品实现步骤示例

在阶段 A 中完成基本产品的需求和概念设计之后，需要检查以确保它们是可以实现的。注意：有两类产品。第一类产品是将实际交付给最终用户的“目标产品”。第二类的产品称为“阶段产品”。阶段产品是在特殊的寿命周期阶段产生的，用来辅助项目最终产品的开发。例如，在 A 前阶段，可以建立一个内充泡沫模型以帮助某些概念的形象化。这些实物模型不是“最终目标产品”，而是“阶段产品”。对于本例的阶段 A，假设要建立关键概念的计算机模型进行仿真，以证明它们是可以实现的。这些模型就是本例的阶段产品。

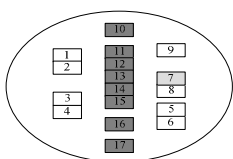
现在的重点转移到系统工程引擎右侧的流程（即产品实现流程），从产品的最底层开始向上递归应用。

1. 第一步

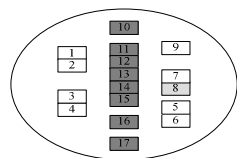


在产品树中，每个底层（图 2.3-6 中无阴影部分）的阶段产品（本例的计算机模型）独自实现（即可以购买、建造、编码或重用）。在本例中，假设外部燃料箱产品模型 Aa 是购买现货产品。产品 Aba 重用其他项目的模型，而产品 Abb 是一个必须在组织内部设计和开发的模型。

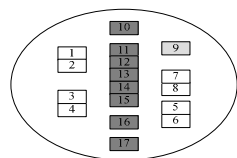
注意：这些模型是一个在系统工程引擎后续步骤中需要组装和集成到更大模型产品的组成部分。也就是说，为了实现外部燃料箱中产品 Ab 的模型，需要首先建立产品 Aba 和 Abb 的模型并进行集成。系统工程引擎的这一过程反映了其实现部分。同样，其他无阴影的底层模型产品也在第一步实现。这些模型将有助于了解和计划实现目标产品的方法，并确保实施方法的可行性。



随后，每个实现的模型（阶段产品）被用于验证目标产品能否满足在产品系统设计步骤中由技术需求定义流程明确的产品需求。这表明通过试验、分析、检查和演示验证，该产品可能满足分配、派生或生成的“需要”陈述，即产品能够“正确制造”。每个无阴影底层模型产品都需要验证。注意：在阶段 A，各步骤的流程不是目标产品的正式验证。不过，使用分析、仿真、模型或其他手段能够显示需求是否合理（可验证），以及概念设计满足需求的程度。这里也允许开发关键领域的验证程序。然而，需要正式验证的是阶段产品（模型）能否满足模型的需求。

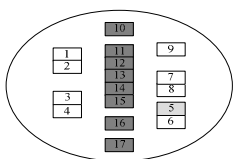


在完成阶段产品（模型）验证及完成用于目标产品的验证规划后，模型需要进行确认。也就是说，执行附加的试验、分析、检查或演示，以确保阶段产品和目标产品的概念设计将有可能满足利益相关者的期望。这将回溯到前述产品系统设计步骤中经过利益相关者期望定义流程与利益相关者协商提出的运行使用构想，并有助于确保在这一层级上项目“建造正确”产品。

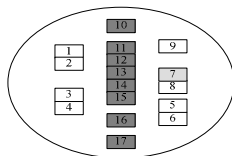


在完成阶段产品（模型）验证和确认并据此规划目标产品验证和确认之后，准备把模型提交到上一层级。根据模型提交的复杂性和安全性需求等，提交形式包括装箱货运、网络传输或随身携带到上一层级的实验室。只要可能，每个底层产品模型都应准备好并提交到上一层级进行集成。

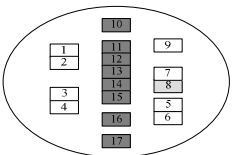
2. 第二步



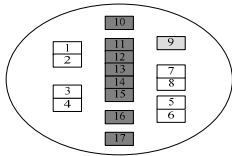
目前,所有底层目标产品的模型(阶段产品)已经被实现、验证、确认和交付,可以开始将它们集成到上层产品中。以外部燃料箱为例,在第4层实现的产品Aba和Abb的模型可以集成为第3层产品Ab的模型。注意:产品实现流程只发生在最底层的产品。系统工程引擎的所有后续步骤将调用产品集成流程,把已实现的产品集成为新的高层产品。集成低层的阶段产品将产生较高层的阶段产品。这种集成流程也可用于实现顶层目标产品的集成。



较高层的新的阶段产品(模型)集成后(如第3级产品Ab),必须证明该产品满足需求。对于这个集成产品模型来说,应当满足在前述系统设计步骤中由技术需求定义流程开发确定的分配需求、派生需求 and 新生需求。这确保集成产品的正确制造(组装)。注意:仅验证集成过程中的组件部分(即单个模型)不足以认定集成产品能够正常运行。这样可能会发生各方面的问题——如接口方面的需求不完整、设计期间的错误假设等。确定集成产品完好的唯一方法是在每个层级进行验证和确认活动。验证集成阶段产品所获得的知识也可用于规划最终顶层产品的验证。

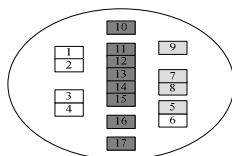


同样,在集成阶段产品验证后,需要确认其满足运行使用构想文件中明确的对该层产品模型的期望。即使此时构成集成产品的组件部分通过确认,也必须进行对集成产品自身的确认,如此才能保证项目建立了“正确的”集成产品。这些确认信息同样将有助于规划最终顶层产品的确认活动。



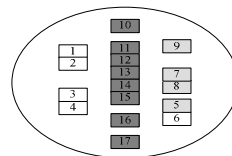
当前层次的集成阶段产品模型(如第3层产品Ab)已准备好提交到上一层次(如第2层)。与第一步中的产品相同,集成阶段产品已根据其需求/要求准备好并运送或提交。在本例中,外部燃料箱的第3层集成产品Ab的模型被提交到第2层产品A的模型所有者中。这个阶段产品移交工作有助于规划目标产品的交付活动。

3. 第三步到第n步



与第二步的方法类似,第3层产品模型经过集成、实现、验证、确认,并移交到上一层次。在本例中,外部燃料箱第3层集成阶段产品Ab和Aa的实现模型集成形成第2层阶段产品A。注意:第3层产品Aa是集成流程中的最底层产品。它可能在某个较早时刻已经实现,等待产品Ab的实现。产品Aa移交的部分可能已经安全存储,直到Ab的相关产品可用,也可能Aa需花费较长时间而Ab在某个较早时刻已经完成,并等待购买的Aa到达从而共同完成集成。产品树分支的长度不必转换为相应的时间长度。这就是为什么在项目最早阶段做出良好规划是如此的关键。

4. 最终步骤



在某种程度上,所有第一层阶段产品的模型都被用于确保阶段A中提出的系统需求和构想能够得以实施、集成、验证、确认和交付。本例中定义该层单元为外部燃料箱、轨道器和固体火箭助推器。通过系统工程引擎的最后步骤将显示这些单元能够成功地实现、集成、验证和确认。

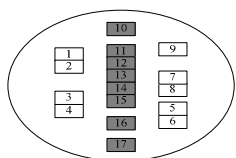
这些产品最终将以系统需求、运行使用构想、概念化功能和物理设计的控制基线形式进入寿命周期的阶段 B，并得以进一步完善。在后面的阶段中，这些产品将真正以实物形式实现。在项目各个阶段中，每个产品的主要特征通过关键系统工程文档传承下去。

2.3.2.3 系统工程引擎中阶段 B 到 D 的使用示例

阶段 B 开始进行目标产品的初步设计。系统工程引擎的递归步骤以类似阶段 A 中详细讨论的方式来重复执行。在这个阶段，阶段产品可能是该产品的原型。原型完成开发并通过有计划的验证和确认程序来确保设计能接近满足最终飞行器建造之前所有的需求和期望。在原型中找到各类错误并更正要比在飞行器实际建造和合格检验时找到错误并更正更加容易且花费更少。

相对于前面阶段以分析、构想和原型的方式研究目标产品，阶段 C 和阶段 D 直接针对目标产品开展工作。在阶段 C 中，递归使用系统工程引擎的左侧流程进行详细设计。在阶段 D 中，递归使用系统工程引擎右侧流程实现最终产品，并进行正式验证和确认。在完成系统工程引擎阶段 D 最后一步之后，得到完整实现的目标产品 STS，并可随时交付发射使用。

2.3.2.4 系统工程引擎中阶段 E 到 F 的使用示例



即使在寿命周期的阶段 E（使用与维护）和阶段 F（退役处置），系统工程引擎技术管理流程仍在使用。在项目的运行使用阶段，多数活动仍在进行。除了产品的日常使用，还有必要的监督或管理系统的各个方面。早期开发阶段提出的关键技术性能指标在这里继续发挥作用（技术性能指标在第 6.7.2 节进行描述）。这些重要的监测指标确保产品按照设计和预期运行。系统技术状态仍在控制范围内，技术状态管理流程仍在执行，仍然通过决策分析流程进行决策。事实上，所有技术管理流程仍在应用。在本例的讨论中，术语“系统管理”被用于系统运行的技术管理方面。除了系统管理和系统运行，也可能需要定期翻新、修理、清洁、清理、配送或其他活动。虽然也可使用其他术语，但针对本例讨论，使用术语“维护工程”来表示这些活动。同样，所有技术管理流程仍然适用于这些活动。图 2.3-7 表示这三个活动在最终产品的运行周期内同时和连续发生的模型。系统工程流程中的某些部分需要不断进行，甚至在系统不再运行而停用、退役和处置后仍进行。这符合系统工程“自始至终”掌控系统全寿命周期的基本原则。

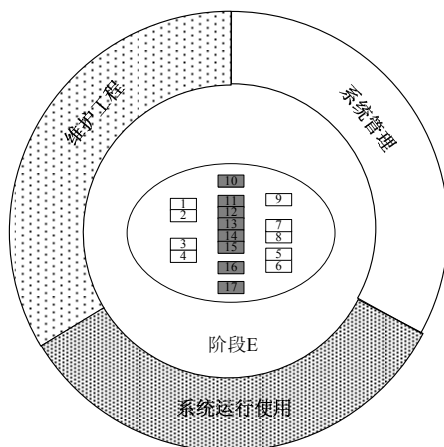


图 2.3-7 产品阶段 E 的典型活动模型

如果在本阶段开发新产品，或需要做出影响产品设计和验证的变更，或需要对现有产品进行升级，产品开发过程应返回系统工程引擎顶部重新开始。也就是说，升级的第一件事是确定利益相关者和他们的期望。完整的系统工程引擎仅用于新产品开发，如图 2.3-8 所示。注意：图中的系统工程引擎虽然只显示一次，但对升级产品却是按产品层次递归调用，如同前面产品详细示例所描述。

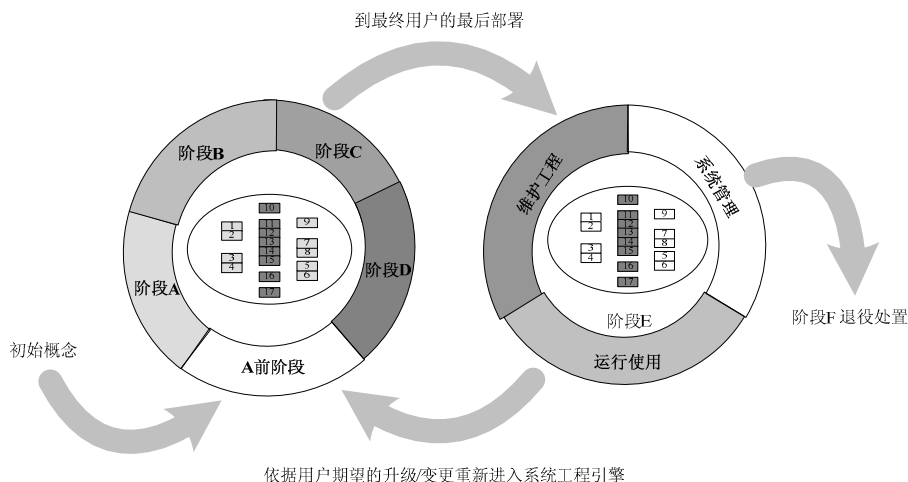


图 2.3-8 新产品或升级产品重新进入系统工程引擎

2.4 产品验证和产品确认的区别

从流程角度来看，产品验证流程和产品确认流程的性质类似，但它们的目标不同。产品的验证是为了证明产品符合要求，即通过试验、分析、检查或演示来证明产品满足每个按“需要”陈述的需求。产品的确认则是为了证明产品能够在特定的环境中实现预期的目标，即通过试验、分析、检查或演示来证明产品满足客户和其他利益相关者的期望。

验证试验与已批准的需求集相关，并且能够在产品寿命周期的不同阶段实施。被批准的规范、图纸、部件清单，以及其他技术状态文件确立该产品的技术状态控制基线，这些技术状态控制基线在后续阶段可能需要修正。没有经过控制基线的验证和适当的技术状态控制，后续阶段修正可能代价高昂且易导致严重的性能问题。

确认试验则与运行使用构想文件相关。对目标产品的确认试验在现实条件（或仿真条件）下进行，以确定将产品用于使命任务运行时的有效性和适用性。

验证和确认的方法基于工程技术进行判断选择，这种工程技术判断是表明产品是否符合要求或者是否像运行使用构想中计划和描述的那样是最有效方法。

2.5 系统工程的费用

系统工程的目的是在充分考虑性能、费用、进度和风险等因素的基础上设计、建造和运行使用系统，使系统以最具效益的方法安全实现其目标。

一个经济有效的和安全的系统必须在效能和费用之间取得特定的平衡：当消耗的资源相同

时，系统必须能够获得最大效能；同样当获得的效能相同时，系统必须消耗最少的资源。这是一个弱约束条件，因为通常有许多设计符合该条件。将每个可能的设计看做效能和费用权衡空间内的一个点。通常，画出在当前技术条件下设计所能达到的最大性能与费用的函数关系曲线，得到如图 2.5-1 所示的图形（图中，纵坐标（Y 轴）代表效能尺度，横坐标（X 轴）代表费用尺度）。换言之，曲线描述出在当前的技术条件下能够实现的设计方案的费用效能包络曲线。

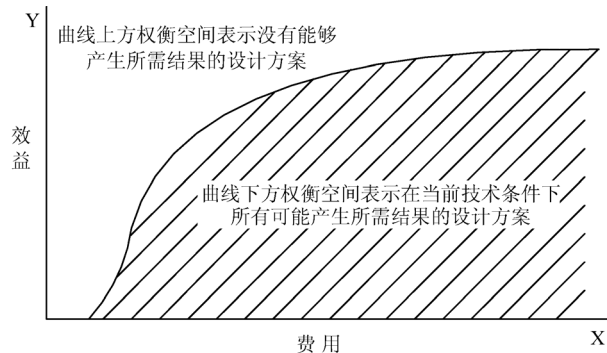


图 2.5-1 非劣方案的包络线

曲线上的点是当前技术条件下不能达到的，也就是说，它们代表的设计是不可行的（其中某些点在未来技术进一步发展之后可能会变成可行的点）。包络线以下的点是可行的，但与费用效能点落在包络线上的设计相比处于劣势。包络线上的点代表的设计被称为经济有效的解决方案。

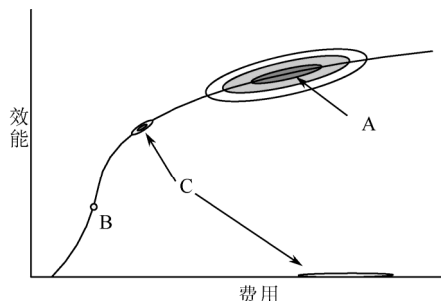
设计权衡研究是系统工程流程的重要部分，往往试图在不同费用和效能组合的设计中寻找更好的设计。当权衡研究的起点在包络线以内时，得到的设计方案或在整体效能不减的条件下降低费用，或在保持费用不增的情况下增加效能（即向包络线接近）。这样，系统工程师就很容易做出决定。像设计子系统的尺寸这样“双赢”的设计虽不常见，但绝非罕见。当设计方案权衡研究中需要在效能和费用之间权衡，或权衡相同费用下的效能（即水平方向移向包络线），做出决定会更加困难。

系统费用、效能和费效比

- **费用：**系统的费用是指设计、建造、运行和处置系统所需资源的计算值。由于资源的形式多种多样（NASA 工作人员和承包商的工作、材料、能源，以及风洞、厂房、办公室、计算机等设施），因而使用统一货币形式（如指定年代的美元）衡量资源的价值将会非常方便。
- **效能：**系统的效能是系统能够实现目标程度的定量描述。效能的度量通常很大程度上依赖于系统的性能。例如，运载火箭的效能取决于成功地将有效载荷发射到运行轨道的概率。相应系统性能因素包括送入指定常规轨道的有效载荷质量，以及在载荷质量、发射速度和发射有效性之间的权衡。
- **费效比：**系统的费效比是与系统目标相关的费用和效能的联合度量。虽然作为不同的取值分别描述它们是有必要的，但有时在设计优化中也需要将它们组合成一个更有意义的、单值的目标函数。即使不知道如何权衡效能和费用，通常也会首选那些成本较低而效能较高的设计。

寻找最佳效益设计的过程因为不确定性而变得更为复杂，如图 2.5-2 所示。某一特定系统将得到什么输出结果是不可精确预知的，因此，使用单值点描述项目设计的费用和效能最

好用概率分布替代。这种概率分布可以理解为一种“云”，在最大可能取值处“云”的厚度最大，而距离最大可能取值处越远，“云”的厚度就越薄，如图 2.5-2 中 A 所示的设计。不



注意：A、B、C 是不同风险类型的设计方案

图 2.5-2 来源于含有不确定性设计方案的结果估计

确定性很小的设计对应的分布结果，是高密度和高度紧凑的“云”，如图 2.5-2 中 B 所示的设计。还有存在风险的设计，有很大可能产生令人不满意的结果，如图 2.5-2 中 C 所示的有一个附加的低效能，高成本设计对应的“云”（当然，这种“云”的包络不会像图中那样界线明显，而是相当模糊的。边界线可看做是在某一置信水平下的包络线，即达到相应效能值的给定数值概率）。

效能和费用可能需要多种描述方法。效能方面如 Echo 气球（约 1960 年），除了完成作为通信卫星的主要任务之外，还需要获取电磁环境和大气阻力的科学数据。此外，Echo 气球作为最早肉眼可见的卫星，本身就具有无可估量的效能，但这在空间竞赛的初期并不被认可。又如 Sputnik*（1957 年）作为事实上的第一颗人造卫星，其效能体现在多个方面。作为有限资源支出的费用，可以通过资金、人员、设施的使用等方面来度量。进度可以作为效能或成本的属性或约束条件。火星探索的使命任务如果错过发射窗口就必须等待约两年后的另一次机会——这是明显的进度约束实例。

某些情况下，在固定预算和固定风险范围内寻找可能的最大效能较为合适，而在其他情况下，寻求给定效能和风险下可能的最低费用更适合。对于这些情况，问题是如何指定效能水平或如何确定费用水平。实践中，这些指标可以根据性能和费用要求来确定。这样问题就适当地转换为略微放松效能要求能否使得系统费用显著减少，或增加少许资源能否使得系统效能显著提高。

技术团队必须在属性描述各不相同的众多设计之间进行选择。目前，已开发出多种方法来帮助确定属性的参数选择和利用相对价值量化主观评价之间的偏好。这样做之后，属性权衡就可以定量评估。但是，经常会发生属性并不适合的情况，这时就要针对属性多样性做出决策。

系统工程师面临的困境

对于每一个经济有效的解决方案：

- 保持风险不变，减少成本，性能一定会降低。
- 保持成本不变，减小风险，性能一定会降低。
- 保持性能不变，减少成本就会造成风险提高。
- 保持性能不变，减少风险就会造成成本提高。

在这种情况下，时间进度往往是一种关键资源，因而进度起到一种成本的作用。

* Sputnik：前苏联发射的人类第一颗人造地球卫星（“伴侣号”），于 1957 年 10 月 4 日由前苏联的 R7 火箭在拜科努尔航天中心发射升空。

第3章 NASA 工程/项目寿命周期

NASA 在大型系统管理中的一个最基本概念是工程/项目寿命周期，把工程或项目中需要实现的所有事项划分为若干明显的阶段，并由关键决策点区分。关键决策点是指决策机构确定工程/项目进入寿命周期下一阶段（或者下一个关键决策点）是否准备就绪的事件点。定义寿命周期阶段边界，可以为系统提供确定是否通过的自然决策点。决策权依据系统所处阶段的相关处置权确定，该权利必须在约定时间内移交。工程或项目未通过关键决策点评审可能需要“归零重新开始”或者可能被终止。

所有系统起源于对其必要性的认识或对其机遇的发现，并通过多个不同的开发阶段达成最终的成果。与系统工程相关的分析和优化活动，其最有决定性的影响产生于系统的早期阶段，这些产生价值数百万美元成本影响的决策活动将在系统开发过程中持续进行，直到系统寿命周期的终结。

将工程/项目寿命周期分解为阶段，可以将整个过程划分成更易管理的部分来进行组织。工程/项目寿命周期为管理者提供不断增加的可视性，使其能够了解在管理和预算环境相应的时间点上系统的进展。

NPR 7120.5《NASA 空间飞行工程和项目管理需求》将 NASA 寿命周期阶段定义为规划论证与实施执行两个阶段。对飞行系统和地面保障项目，NASA 寿命周期的上述两个阶段又分为以下 7 个递进阶段。

- **A 前阶段：**概念探索（即确定可行备选方案）。
- **阶段 A：**概念研究和技术开发（即项目定义，明确和组织必要的技术）。
- **阶段 B：**初步设计和技术完善（即建立初步设计方案，开发必要的技术）。
- **阶段 C：**详细设计和制造（即完成系统设计，进行组件的建造/编码）。
- **阶段 D：**系统组装、集成、试验和投产（即集成组件，验证系统，系统投入生产并准备运行使用）。
- **阶段 E：**运行使用与维护（即运行与维修系统）。
- **阶段 F：**退役处置（即处置系统，分析数据）。

图 3.0-1 和图 3.0-2 分别标识 NASA 工程寿命周期和 NASA 项目寿命周期关键决策点，描述各阶段特征。3.1 节和 3.2 节阐述 NASA 工程寿命周期阶段的目标、主要活动、产品和关键决策点。3.3 节~3.9 节阐述 NASA 项目寿命周期阶段的目标、主要活动、产品和关键决策点。3.10 节描述 NASA 工程/项目负责人和系统工程师必须执行的预算周期。

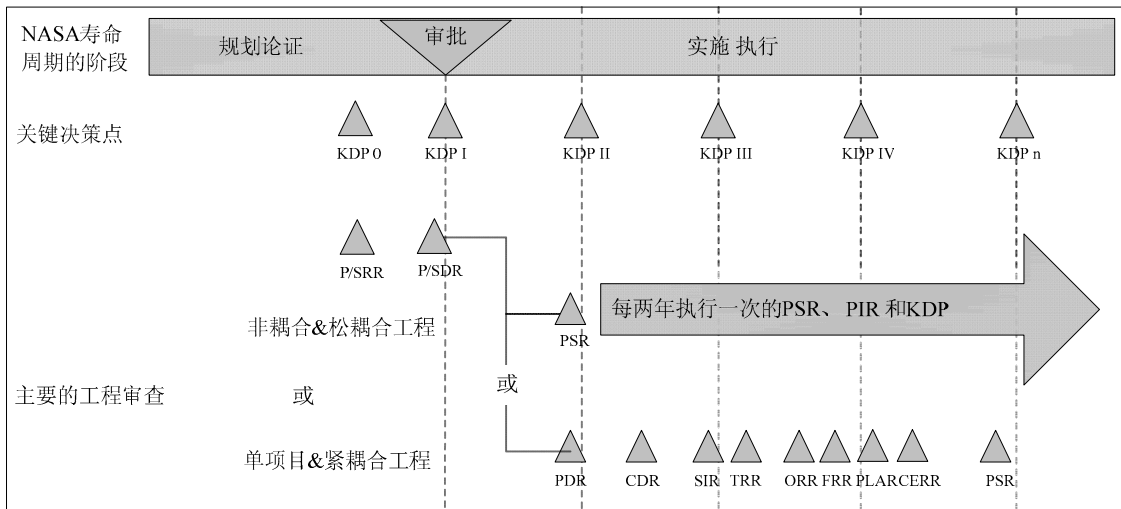


图 3.0-1 NASA 工程寿命周期

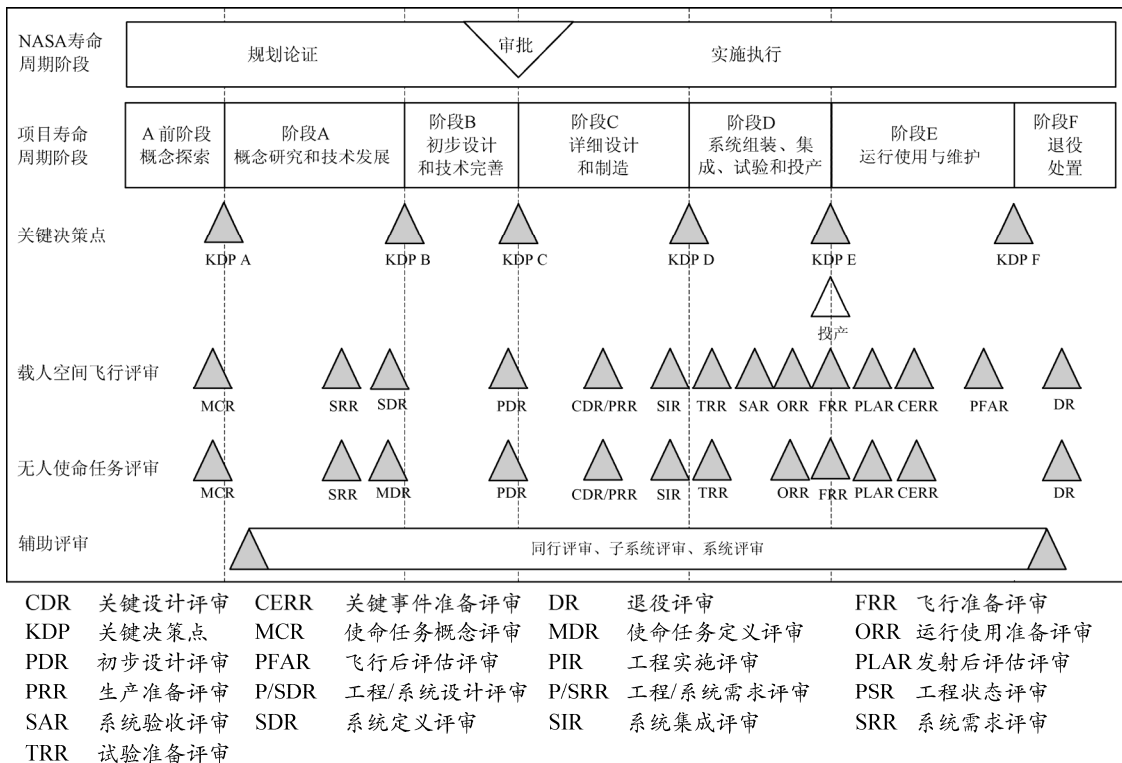


图 3.0-2 NASA 项目寿命周期关键决策点

3.1 工程规划论证

工程规划论证阶段形成一个确实能够满足 NASA 总局和使命任务主管部门目的和目标的经济有效的工程立项。

工程规划论证授权文件批准工程负责人启动新工程的计划工作，并进行必要的分析从而形成合理的计划。关键决策点 I 进行的评审决定工程的审批，包括工程/系统需求评审、工程/系统设计评审（工程/系统设计评审）、工程审批评审，以及工程管理委员会的评审（见图 3.0-1 和图 3.0-2）。工程规划论证阶段需要的门户产品的概要可参阅 NPR 7120.5。

所有类型工程的规划论证阶段是一致的，包括一个或者多个在关键决策点 I 所需进行的评审，最终做出批准工程开始实施执行的决策。通常，在其首要项目做好实施执行准备之前，工程不能进入实施执行阶段。

工程规划论证

目的

建立有成本效益的工程，使之确实能够满足 NASA 总局和使命任务主管部门的目标和目的。

典型活动及其产品

- 开发工程需求并分配到初始项目。
- 明确并批准工程采办策略。
- 开发与其他工程的接口。
- 启动工程中多个项目交互关联技术的开发。
- 得出初始成本估算，批准工程预算。
- 开展 NPR 7120.5 中定义的工程规划论证必要的技术活动。
- 满足 NPR 7123.1 中规定的工程规划论证评审启动/成功准则。

评审

工程/系统需求评审。

3.2 工程实施执行

在工程实施执行阶段，项目负责人与使命任务主管助理，以及相关项目负责人共同工作，来执行以高成本效益为目标的工程计划。

在经费约束下工程评审确保工程持续有助于达成 NASA 总局和使命任务主管部门的目标和目的。工程实施执行阶段需要的门户产品的概要可参阅 NPR 7120.5。

根据工程类型，工程寿命周期有两个不同的实施执行途径。每种实施执行途径有不同的主要评审类型。

对项目相对独立的或者联系不紧密的工程，实施执行阶段仅要求进行工程状态评审和工程实施情况评审以评估工程绩效，并大约每两年提出进行关键决策点评审的授权建议。仅单一项目和项目紧耦合的工程比较复杂。对于单一项目的工程，图 3.0-1 所示的实施执行阶段工程评审与项目寿命周期内直到阶段 D 的项目评审（见图 3.0-2）含义相同（但不重复）。偶尔在实施中，此类工程同样进行两年一次的伴随工程状态评审/工程实施情况评审的关键决策点评审。紧耦合工程实施执行期间与项目评审紧密联系，以确保项目能够相应集成为更大的系统。偶尔在实施中，紧耦合工程同样进行两年一次的工程状态评审/工程实施情况评审/关键决策点评审，以评估工程绩效并批准其延续。

工程实施执行

目的

实施执行工程和相应项目，确保工程在经费约束下持续有助于达成 NASA 总局的目标和目的。

典型活动及其产品

- 通过直接分派或竞争过程启动项目（如发布投标指南、商机公示）。
- 监控工程论证、审批、实施、集成、运行及最终退役处理。
- 根据资源和需求变更调整工程。
- 根据 NPR 7120.5 开展必要的工程实施执行阶段的技术活动。
- 满足 NPR 7123.1 中规定的工程实施执行评审的启动/成功准则。

评审

- 工程状态评审/工程实施情况评审（仅对非耦合或松耦合工程）。
- 评审与项目寿命周期内直到阶段 D 的项目评审（见图 3.0-2）含义相同（但不重复）（仅针对单一项目和紧耦合工程）。

3.3 项目 A 前阶段：概念探索

该阶段目的是谋划可行概念，由此选定新的工程/项目，通常由概念研究团体不间断地进行。一般来说，该阶段活动包含对新观点宽松的结构检验，通常没有集中控制，且大多是一些较小的研究项目。该阶段主要产品是项目建议清单，这些建议是对符合 NASA 使命任务、能力、重点项目和资源约束的需求辨识和商机发现。

预先研究可能持续多年，并可能最终只是一些松散相关的文件。

这些研究通常集中在建立使命任务目标和构建顶层系统需求及运行使用构想。通常给出概念设计以演示验证可行性并支撑工程性估算。概念探索强调立项的可行性和迫切性而非最优化。可选的分析和设计手段相应深度和数量上是有限的。

A 前阶段：概念探索

目的

为完成使命任务提出广泛的想法和方案，从而可以选定新的工程/项目。

典型活动和产品

（注意：商机公示项目中应已经定义可交付产品）。

- 根据许可文件识别使命任务和工程架构。
- 识别并确定用户和其他利益相关者。
- 确定并执行权衡和分析。
- 确定需求如下：
 - 使命任务；
 - 科学技术；
 - 顶层系统。
- 定义效能指标和性能指标。
- 确定顶层技术性能指标。
- 初步评估可能的使命任务。
- 准备工程/项目建议如下：
 - 使命任务判定和目标；
 - 可能的运行使用构想；
 - 高层级工作分解结构；
 - 费用、进度和风险估计；
 - 技术评估和技术成熟策略。
- 准备初步使命任务概念报告。
- 执行 NPR 7120.5 规定的 A 前阶段必需的技术活动。
- 满足 NPR 7123.1 规定的使命任务概念评审启动/成功准则。

评审

- 使命任务概念评审。
- 非正式建议的评审。

3.4 项目阶段 A：概念研究和技术开发

阶段 A 的活动是完整地开发控制基线明确的使命任务概念，并安排或确保所需技术开发的责任。这项工作及与利益相关者的交互，能够帮助建立使命任务概念和工程对项目的需求。

在阶段 A，通常由一个与工程办公室或非正式的项目办公室相关的开发团队重新陈述使命任务概念，以确保项目的合理性和实用性，以及能够在 NASA 的预算中得到充分保证。

开发团队的工作集中于分析使命任务需求并建立使命任务架构。活动是正式的，重点从原先的可行性转向最优性。工作面更加深入并考虑众多的备选方案。

目的和目标是不变的，项目在系统需求、高层系统架构，以及运行使用构想方面开发更多定义。概念设计已开展，并较概念研究展示出更多的工程技术细节。技术风险识别更加详细，同时技术开发需求成为焦点。在阶段 A，工作重点在于将系统功能分配到特定的硬件、软件和人员等。

在努力获取更经济有效的设计中，通过系统权衡和子系统权衡的反复进行，系统功能和性能需求，连同架构和设计，变得更加稳定（权衡研究应在系统设计决策之前而非之后进行）。该阶段的主要产品包括已接受的系统功能控制基线及主要的系统目标产品。同时提出各种工程技术及管理计划，以准备管理项目的后续流程，如验证和使用，准备开展专业工程技术工作。

阶段 A：概念和技术开发

目的

确定所提出重大新系统的可行性和迫切性，并建立与 NASA 战略规划兼容的初始控制基线。

典型活动及产品

- 准备并启动项目计划。
- 开发顶层需求和约束。
- 定义和归档系统（硬件和软件）需求。
- 将初步系统需求分配到较低层次。
- 明确系统软件功能描述和需求。
- 明确并说明内部和外部接口需求。
- 确定综合后勤保障需求。
- 开发相应的评价准则和指标。
- 归档运行使用构想。
- 确定使命任务概念报告基准。
- 演示验证设计的可信性和可行性。
- 开展并完成权衡研究。
- 开发使命任务架构。
- 启动环境评估/国家环境政策法规流程。
- 开发初始轨道碎片评估方案（NASA 安全标准 1740.14）。
- 建立技术资源评估。
- 定义寿命周期费用评估与开发系统层级费效模型。
- 定义工作分解结构。

- 开发完成系统任务书。
 - 获取系统工程工具和模型。
 - 确定系统工程管理计划控制基线。
 - 开发系统风险分析方案。
 - 准备并启动风险管理计划。
 - 准备并启动技术状态管理计划。
 - 准备并启动数据管理计划。
 - 准备工程技术专业计划（如污染物控制计划、电磁干扰/电磁兼容控制计划、可靠性计划、质量控制计划、部件管理计划）。
 - 准备安全性和使命任务担保计划。
 - 准备软件开发和管理计划（参考 NPR 7150.2）。
 - 准备技术开发计划并启动先进技术开发。
 - 建立人力资源评价计划。
 - 定义验证和确认的方法，并在验证和确认计划中归档。
 - 开展 NPR 7120.5 中要求的阶段 A 技术活动。
 - 满足 NPR 7123.1 中阶段 A 的评审启动/成功准则。
- 评审
- 系统需求评审。
 - 使命任务定义评审（仅针对无人飞行任务）。
 - 系统定义评审（仅针对载人空间飞行）。

3.5 项目阶段 B：初步设计和技术完善

在阶段 B 中，主要活动是（根据 NPR 7120.5 和 NPR 7123.1）建立初始的项目控制基线，包括“飞行和地面单元的项目层性能需求正式分解为完整的系统和子系统设计规范集”及“相应的初步设计”。技术需求应该充分详细，以建立可靠的项目进度和费用估计。

还应注意，对于商机公示项目，阶段 B 的作用就是在技术状态控制下，最终确定和处理顶层需求及向下层分解的需求。

尽管在阶段 A 确定需求控制基线，在阶段 A 后期和阶段 B 早期仍不可避免地有相当多由权衡研究和分析导致的变更。然而，在阶段 B 中期，顶层需求应该完全确定。

实际上，阶段 B 的控制基线由覆盖项目技术和商务方面的演化的控制基线汇总组成，包括系统（及子系统）需求和规范、设计、验证、使用计划等控制基线的技术部分，以及进度、费用规划和管理计划等商务部分。控制基线的确定意味着技术状态管理技术规程的实施（参见 6.5 节）。

在阶段 B 中，工作重点转移到建立功能完备的初步设计方案（即功能控制基线），以满足使命任务目标。权衡研究继续进行。目标产品的主要接口已定义。工程试验产品可能已制成并用于获取进一步设计工作所需的数据，而项目风险通过成功的技术开发和演示验证得到缩减。

阶段 B 在一系列的初步设计评审（包括系统层初步设计评审和适当时针对低层级目标产品的初步设计评审）后结束。初步设计评审反映需求的不断细化直到设计完成（参见 4.4.1.2 节和图 4.4-2 对持续细化的讨论）。初步设计评审揭示的设计问题需要解决，这样使详细设计能在明确的设计规范下开始。从这一点看，几乎所有控制基线变更都期望反映设计的持续细化，而非根本上的变更。在确定控制基线之前，系统架构、初步设计，以及运行使用构想必须经过充分的技术分析和设计工作确认，建立比阶段 A 更详细的可信和可行的设计方案。

阶段 B：初步设计和技术完善**目的**

足够详细地定义项目，建立能够满足使命任务需求的初始控制基线。

典型活动及其产品

- 确定项目计划控制基线。
- 评审并更新阶段 A 开发并确定控制基线的文档。
- 基于成熟的运行使用构想开发科学/探索方面的运行使用计划。
- 更新工程技术专业计划（如污染物控制计划、电磁干扰/电磁兼容控制计划、可靠性计划、质量控制计划、部件管理计划）。
- 更新技术成熟度计划。
- 报告技术开发结果。
- 更新风险管理计划。
- 更新成本和进度数据。
- 确定并批准顶层需求，将需求向下层分解。
- 建立并确定（硬件和软件）设计规范和设计图，验证和确认计划，低层接口文档的控制基线。
- 开展权衡研究并达成结果。
- 开展设计分析并报告结果。
- 进行工程技术开发试验并报告结果。
- 选择控制基线的设计解决方案。
- 确定初步设计报告控制基线。
- 确定内部和外部接口设计解决方案（如接口控制文档）。
- 确定系统运行使用，以及性能指标/合同申请的管理、评审、访问和应急计划。
- 开发相应层次的安全性数据包。
- 初步开发的轨道碎片评估。
- 开展 NPR 7120.5 中规定的阶段 B 必要的技术活动。
- 满足 NPR 7123.1 中阶段 B 评审的启动/成功准则。

评审

- 初步设计评审。
- 安全性评审。

3.6 项目阶段 C：详细设计和制造

在阶段 C 中，主要活动是建立完整的设计方案（配定控制基线）、进行硬件产品制造或生产及软件编码，为产品集成做准备。权衡研究继续进行。完成更接近真实硬件的工程试验单元的制造和试验，以确定设计的系统在预期运行环境中功能正常。工程技术专业分析结果集成到设计中，且制造过程和控制得到有效说明和确认。所有在阶段 A 后期针对试验和运行设备、流程和分析、工程技术专业分析集成、制造过程和控制而启动的计划已经实施。在完成详细接口的定义后，技术状态管理持续跟踪并控制设计的变更。在详细设计逐步细化的每一步，将更加详细地计划相应集成和验证活动。在这一阶段，技术参数、进度和预算被密切跟踪，以确保能够及早发现不良趋势（如空间飞行器质量的意外增加或其成本增长）并采取纠正行动。这些活动的重点是准备关键设计评审、生产准备状态评审（若需要）和系统集成评审。

阶段 C 由一系列关键设计评审组成，包括系统层的关键设计评审和对应系统结构不同层次的关键设计评审。每个目标产品的关键设计评审应该在开始制造/生产硬件产品之前和开始对可交付软件产品编码之前进行。通常，关键设计评审的排序反映将发生在下一个阶段的集

成流程——即从底层关键设计评审到系统层关键设计评审的集成。当然，项目应裁剪评审的顺序以满足项目的需要。如果产品投入生产，将实施生产准备状态评审以确保生产计划、设备和人员已做好开始生产的准备。阶段 C 在实施系统集成评审后结束。该阶段的最终产品是准备集成的产品。

阶段 C：详细设计和制造

目的

完成系统及相关子系统（包括操作系统）的详细设计，硬件产品制造及软件编码。

典型活动及其产品

- 更新阶段 B 开发和确定控制基线的文档。
- 更新接口文档。
- 基于成熟的运行使用构想更新使命任务运行计划。
- 更新工程技术专业计划（如污染物控制计划、电磁干扰/电磁兼容控制计划、可靠性计划、质量控制计划、部件管理计划）。
- 拓展已确定控制基线的文档，以反映系统（包括系统架构、工作分解结构和项目计划）成熟度的提升。
- 更新生产计划并确定其控制基线。
- 改进集成技术规程。
- 确定后勤保障计划控制基线。
- 在系统架构中补充增加低层级设计规范。
- 完成制造和组装计划及技术规程。
- 构建待建系统（硬件和软件）规范及图纸、验证和确认计划，以及所有层次的接口文档，并确定其控制基线。
- 确定详细设计报告控制基线。
- 维护需求文档。
- 维护验证和确认计划。
- 根据项目计划监控项目进展。
- 开发验证和确认技术规程。
- 开发硬件和软件详细设计方案。
- 开发系统集成计划及系统运行使用计划。
- 进行全系统的系统信息设计。
- 开发备件计划。
- 开发指令和遥测数据列表。
- 准备发射场检验和使用计划。
- 准备运行和任务激活计划。
- 准备系统退役/处置计划，包括人力资本转移，用于阶段 F。
- 最终确定相应层次的安全性数据包。
- 开发初步运行使用手册。
- 开展权衡研究并达成结果。
- 产品制造（或编码）。
- 在组件或子系统层次上进行试验。
- 把握预先计划的产品升级的时机。
- 确定轨道碎片评估控制基线。
- 开展 NPR 7120.5 中规定的阶段 C 必需的技术活动。
- 满足 NPR 7123.1 中阶段 C 评审的启动/成功准则。

评审

- 关键设计评审。
- 生产准备状态评审。
- 系统集成评审。
- 安全性评审。

3.7 项目阶段 D：系统组装、集成、试验和投产

在阶段 D 中，进行系统组装、集成、试验和投产活动。这些活动重点在于为飞行准备状态评审做准备。活动包括系统组装、集成、验证及确认，包括在留有余量的预定环境中做飞行系统试验。其他活动包括对使用人员的初步培训，以及后勤保障和备件计划的实施。对于飞行项目，活动的重点转移为发射前的产品集成及投产。尽管所有这些活动在项目的阶段 D 进行，但很多活动的计划已在阶段 A 启动。活动计划最晚在阶段 D 开始前启动，因为就满足需求而言项目设计需要大大超前于试验和运行使用。

阶段 D 最终形成能够实现其设计目标的系统。

阶段 D：系统组装、集成、试验和投产

目的

组装和集成产品并建立系统，期间确信其能够满足系统需求，随后进行投产活动并准备运行使用。

典型活动及其产品

- 根据集成和验证计划，将经过验证的组件和子系统集成为成品并进行验证。
- 根据项目计划监控项目进展。
- 在所有层次细化验证和确认技术规程。
- 进行系统合格验证。
- 进行系统验收验证和确认（如涵盖所有单元即空间单元、地面系统、数据处理系统的全系统试验）。
- 进行系统环境试验。
- 评估并审批验证和确认结果。
- 处理解决验证和确认的差异。
- 将所进行的验证和确认结果存档。
- 确定验证和确认报告控制基线。
- 确定已制造硬件产品和已编成软件归档的控制基线。
- 更新后勤保障计划。
- 归档总结的经验。
- 准备并确定运行指南控制基线。
- 准备并确定维护指南控制基线。
- 审批并确定使用手册控制基线。
- 培训首批系统运行操作和维护人员。
- 根据应急计划进行培训。
- 最终确定并实施备件计划。
- 遥感数据确认证实和地面数据处理。
- 证实系统和保障单元已做好飞行准备。
- 与运载火箭集成并发射，实施进入轨道等，最终实现系统部署。
- 实施初始运行使用的验证和确认。
- 执行 NPR 7120.5 中规定的阶段 D 必需的技术活动。
- 满足 NPR 7123.1 中阶段 D 评审的启动/成功准则。

评审

- 试验准备状态评审（针对系统所有层次）。
- 系统验收评审（仅针对载人空间飞行）。
- 运行使用准备状态评审。
- 飞行准备状态评审。
- 系统功能和物理技术状态审核及安全性评审。

3.8 项目阶段 E：运行使用与维护

阶段 E 的活动主要是执行使命任务，满足既定使命任务需求，按需求在使命任务中进行维护和保障。该阶段的产品是使命任务执行结果。这一阶段包括系统的演变，且仅包括不涉及系统架构重大变更的演变。由于演变引起的范围变更构成新的“需求”，项目寿命周期活动需重新开始。对于大型飞行项目，有可能是经过较长时间的飞行，进入轨道后在轨组装并进行最初的调整操作。在主要使命任务即将结束时，项目可以申请使命任务延长，继续相关活动或努力完成额外的使命任务目标。

阶段 E：运行使用与维护

目的

执行使命任务，满足最初确定的需求并根据需求维护保障使命任务。

典型活动及其产品

- 进行运载火箭性能评估。
- 进行在轨空间飞行器检查。
- 激活并应用科学仪器。
- 执行预定的主要使命任务。
- 搜集工程技术和科学数据。
- 培训候补操作人员和维修人员。
- 为未来使命任务阶段培训飞行团队（如行星着陆操作）。
- 维护并审批系统的运行使用和维修日志。
- 维护和升级系统。
- 问题/故障说明报告。
- 处理分析使命任务数据。
- 若获许可则申请使命任务延长，若获批准则进行额外的使命任务活动。
- 按照计划准备系统解效、分解、退役（或根据使命任务的延长确定）。
- 完成飞行后评估报告。
- 完成最终的使命任务报告。
- 执行 NPR 7120.5 中规定的阶段 E 必需的技术活动。
- 满足 NPR 7123.1 中阶段 E 评审的启动/成功准则。

评审

- 发射后评估评审。
- 关键事件准备状态评审。
- 飞行后评估评审（仅用于载人空间飞行）。
- 系统升级评审。
- 安全性评审。

3.9 项目阶段 F：退役处置

阶段 F 的主要活动是实施系统的退役处置计划并分析所有反馈的数据和样本。该阶段的产品是执行退役处置的结果。

阶段 F 在系统完成使命任务后处理系统的退役处置，其发生时刻取决于多种因素。对执行短期使命任务返回地球的飞行系统，其退役处置可能比硬件拆除并返还给所有者要稍微多

一些。对于长期飞行项目，其退役处置可按照既定计划，或因为意外事件（如使命任务失败）而开始。使命任务的终止运行参照 NPD 8010.3《预定退役并终止运行中空间系统及终止使命任务的通告》进行。否则，在技术进步的情况下，系统不论在当前技术状态下还是在改进的技术状态下继续运行都可能造成浪费。为了限制空间碎片，应参照 NPR 8715.6《NASA 限制轨道碎片技术规程需求》提供在其寿命终止时将地球轨道人造卫星从运行轨道移除的说明。对于低地球轨道使命任务，卫星通常脱离轨道。对于小卫星，可以通过轨道缓慢降低直到卫星最终在地球大气层烧毁来实现。对于大型卫星和观测站，必须设计成在受控制方式下衰减或脱轨，这样使它们能够安全地溅落在深海区域。远在 35790 千米高的地球同步卫星事实上几乎不脱离轨道，因此，它们可被推送到更高的轨道，避开拥挤的地球同步轨道。

除了本阶段开始时的不确定性之外，系统安全退役处置的有关活动可能是长期而复杂的，可能影响系统设计。因此，不同的选择和策略，应在工程的早期阶段与相应的成本及风险综合进行考虑。

阶段 F：退役处置

目的

实施阶段 C 中开发的系统退役/处置计划，并分析所有反馈的数据和样本。

典型活动及其产品

- 系统处置和处置过程保障。
- 归档总结的经验。
- 确定使命任务最终报告的控制基线。
- 数据存档。
- 开始人力资源的转移（如果需要）。
- 执行 NPR 7120.5 中规定的阶段 F 必需的技术活动。
- 满足 NPR 7123.1 中阶段 F 评审的启动/成功准则。

评审

退役评审。

3.10 经费：预算周期

NASA 每年从国会获得运营经费。当然，这笔资金来源于持续滚动的预算论证、预算编制到最终预算执行的流程。NASA 的《财务管理需求（FMR）》卷 4 中给出了 NASA 资源组合的预算系统，即规划、计划、预算和执行（PPBE）的概念、目标及总论，并构建了 PPBE 流程的规划和预算编制阶段指南，对 NASA 的预算论证至关重要。《财务管理需求》卷 4 中包含了战略预算规划和资源指南、工程评审、预算编制、预算报告，以及向预算管理办公室（OMB）和国会申辩估算理由的程序。它还提供流程的每个步骤中主要参与者的角色和职责的详细说明。它强化了适用于 NASA 的法律、法规、行政政策和技术规程。典型的 NASA 预算周期高度简化表述如图 3.10-1 所示。

NASA 一般在每年 2 月份结合最新总统预算中做出的经济预测和整体指导方针，编制自身预算。到 8 月底，NASA 完成 PPBE 流程中的规划、计划和预算阶段，并准备向预算管理办公室提交 NASA 初步预算方案。最终 NASA 预算在 9 月份提交到预算管理办公室，并被纳入到总统整体预算中，通常在 1 月份向国会转交。所提议的预算随后经历国会的评审和审批，

向 NASA 授权在国会的约束下使用经费及经费拨付的法案最终获得通过。国会审批程序通常要持续整个夏天。然而近年来，最终的议案往往被推迟到 10 月 1 日新财年开始之后。这些年里，NASA 一直按照国会的决议执行预算。

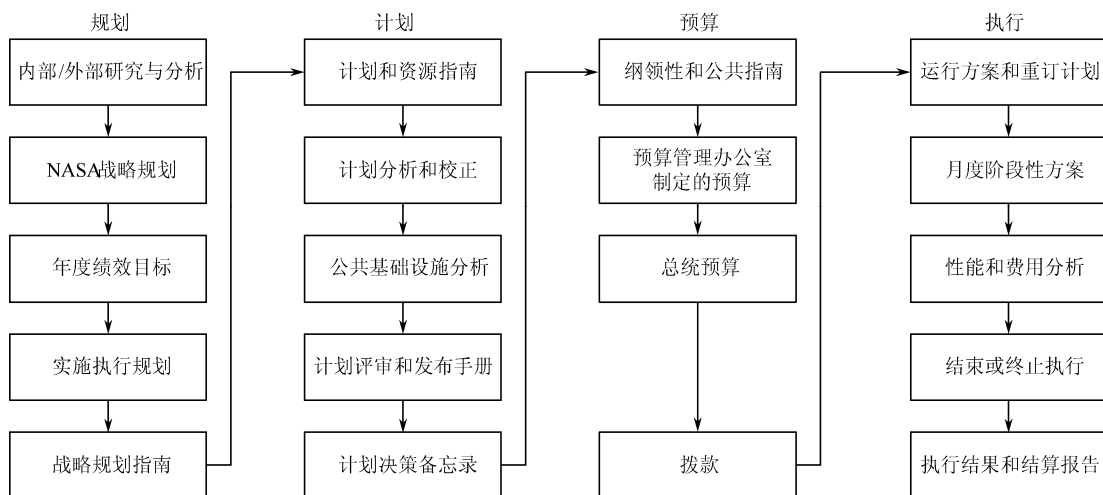


图 3.10-1 NASA 典型的预算周期

在每个财年开始时，年度经费有一个隐含的经费控制门。每年的控制门将规划需求与项目结合，可导致可观的重新规划要求，但它们不属于有序的系统工程流程。相反，它们构成了影响项目风险的不确定性来源之一，因而必须在项目计划中考虑。

第4章 系统设计

本章描述如图 4.0-1 所列系统设计流程中的各项活动。本章按图 4.0-1 所列的步骤 1~步骤 4 划分为相应的小节。每个步骤中的流程按照输入、活动和输出的顺序来讨论。此外，还通过 NASA 项目相关示例提供附加指南。系统设计流程由四个相互依赖、反复迭代和递归的流程构成，最终产生一个满足利益相关者期望的经确认的需求和经确认的设计实现方案。系统设计的四个流程包括明确利益相关者期望、确定技术需求、需求逻辑分解和设计实现方案。

图 4.0-1 说明了系统设计四个流程之间的递归关系。这些流程的起点是由一个研究团队采集并明确利益相关者的期望，包括使命任务目标、约束条件、设计导向、运行使用目标和使命任务成功准则。这组利益相关者的期望与顶层需求用于驱动设计的循环迭代过程，以开发一个粗略的系统架构/设计方案、运行使用构想及派生的需求。这三种产品之间必须保持一致，而为了达到这种一致性需要进行迭代和设计决策。一旦达到一致，项目团队可以通过分析来确认设计是否达到了利益相关者的期望。一个简化的确认要回答如下问题：这个系统能正常工作吗？系统是安全和可靠的吗？系统能在预算和进度约束条件内完成吗？如果这些问题的答案有一个是否定的，则需要变更设计方案或调整利益相关者的期望，相应流程需要重新开始，直到系统（架构、运行使用构想和派生需求）满足利益相关者的期望为止。

设计工作的深度必须足以对设计是否满足需求进行分析验证。当由资深的独立评审小组评定时，设计方案必须是可行的和可信的，且必须足够详细地支持费用建模。

若系统设计满足利益者的期望，研究团队就需要设定产品控制基线并为下一阶段做准备。通常，功能和逻辑分解的中间各层也作为流程的一部分进行验证。在分解的下一阶段，已设定控制基线的派生（及分配）需求变为待分解单元的顶层需求，上述流程重新开始。这些系统设计流程主要应用在 A 前阶段且持续到阶段 C。

A 前阶段的系统设计流程聚焦于产生一个可行的设计，由此使得项目得到正式批准。阶段 A 追求可选的设计方案和附加的成熟度分析以优化设计架构。阶段 B 产生一个能通过立项审批标准的初步设计。阶段 C 完成详细的可生产设计。

以上的简化描述是为了说明系统设计流程的递归关系。这些流程作为指南，根据项目的规模和研究团队的层次结构进行适当剪裁。后面各节针对特定 NASA 使命任务描述四个系统设计流程及其相关产品。

系统设计的关键

- 成功地理解并明确使命任务目标和运行使用构想是获取利益相关者期望的关键，该期望将转化为项目全寿命过程中的产品质量需求。
- 完全和彻底的需求可追溯性是成功确认产品需求的关键因素。
- 清楚和明确的需求将有助于在全系统开发和做出主要或次要变更时避免出现误解。
- 将原始设计构思开发中做出的决策记录在技术数据包中，这样使得初始设计理念和探讨结果可用做评估未来变更和修正的依据。
- 当选定可接受设计方案并将其归档在技术数据包里，该方案将被验证是否满足系统需求和约束条件。当然，设计方案的验证是个持续的反复迭代和递归过程，该过程中不断评价其是否满足利益相关者期望。

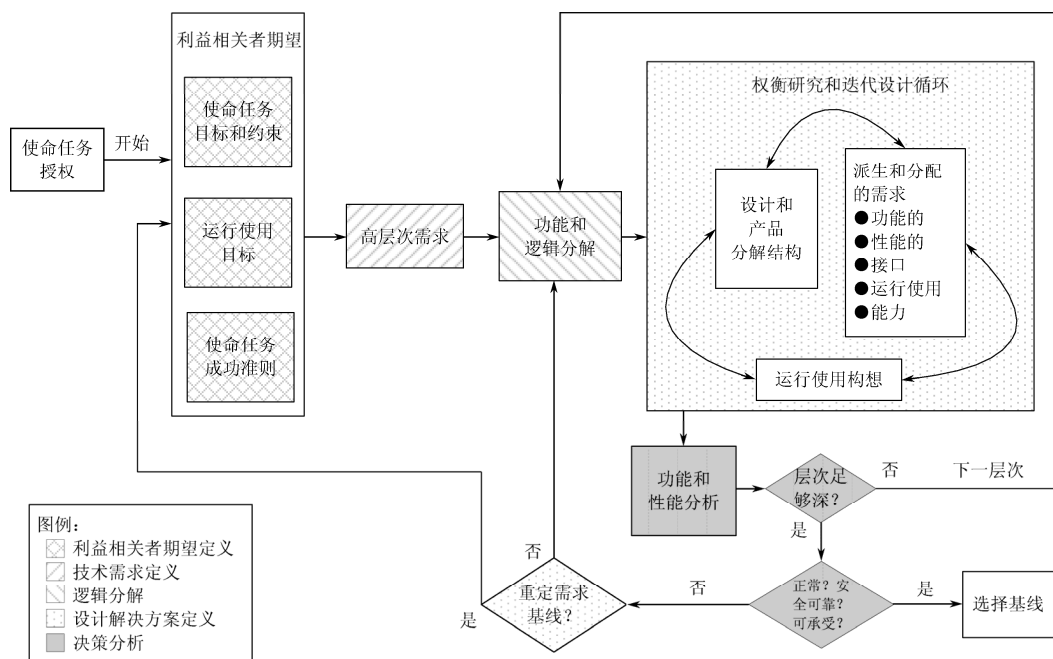


图 4.0-1 系统设计各流程间相互关系

4.1 明确利益相关者的期望

系统工程引擎建立了系统设计与产品实现的基础，而明确利益相关者的期望是系统工程引擎的初始流程。这个流程的主要目的是确认谁是利益相关者，以及准备如何使用产品。这个目的通常通过用例想定、设计参考使命任务和运行使用构想实现。

4.1.1 流程描述

图 4.1-1 提供了明确利益相关者期望的典型流程图，标识了描述明确利益相关者期望流程所考虑的典型输入、输出和活动。

4.1.1.1 输入

明确利益相关者期望流程需要的典型输入包括如下所述。

- **顶层需求和期望：**它们是从更高层（如工程、项目等）向相关特定系统分配的需求和期望（如需求、期望、能力、约束条件、外部接口）。
- **已识别的客户和利益相关者：**对产品有需求及受产品结果影响或某种程度上对产品负责的组织或个人。

4.1.1.2 流程活动

1. 确定利益相关者

新的工程和项目倡议可能来自许多组织、美国总统指示、美国议会、NASA 总部、NASA

中心、NASA 顾问委员会、美国科学学会、美国太空委员会，以及其他科学和太空领域的团体。这些组织通常都可能被认为是利益相关者。利益相关者就是那些受到本项使命任务结果影响或某种程度上对结果负有责任的组织或个人。

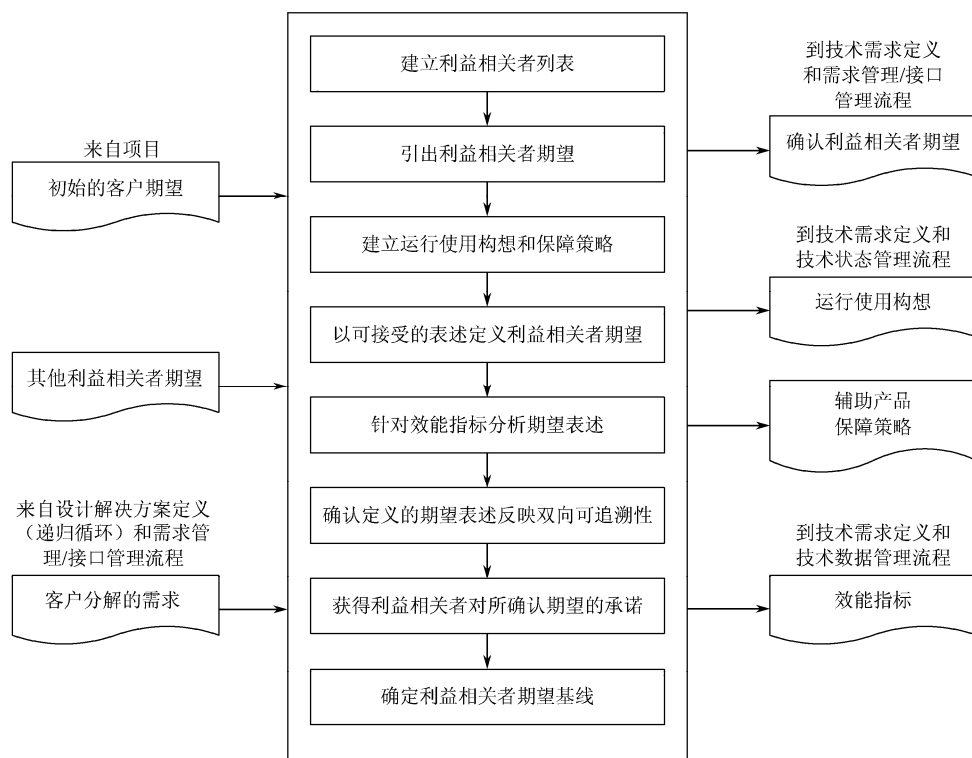


图 4.1-1 明确利益相关者期望流程

利益相关者可以分为客户和其他关注团体（相关利益者）。客户是那些直接接受产品或服务的人，或是直接受益人，例如，科学家、项目负责人和子系统的工程师等。

其他关注团体通过提出宽泛约束对项目施加影响，在这些约束下客户需求必须满足。这些团体可能受项目产品及产品的使用方式影响，或对产品寿命周期保障负责。例如，议会、规划顾问组、工程负责人、使用人员、操作人员、维护人员、使命任务合作方和 NASA 承包商。在这个流程中尽早识别利益相关者非常重要，识别对项目有最重大影响的主要相关利益者同样重要。

2. 确定利益相关者期望

利益相关者期望，即特定的利益相关个人或团体的认识，通过指定所需项目最终状态或目标产品是什么，或为项目目标增加约束范围来确定。这些约束范围可能包括（资源）消耗、交付时间、性能目标，以及其他非定量约束，如组织需求和地缘政治目标。

图 4.1-2 显示了在明确利益相关者期望时需要的信息类型并且描述了信息是如何演化为顶层需求的。曲线箭头描述的是确认路径。图中同时给出了每一步需定义的信息类型实例。

明确利益相关者期望与明确使命任务授权和使命任务战略目标同时开始。使命任务授权随使命任务类型的改变而改变。如科学试验使命任务通常由 NASA 科学使命任务指导委员会的长远规划驱动，而空间探索使命任务则由美国总统直接下令。

明确利益相关者期望的先期工作是理解使命任务目标。清晰描述和记录使命任务目标有利于确保项目团队朝一个共同的目标努力工作。这些目标组成了使命任务开发的基础，所以需要清晰的定义和关联。

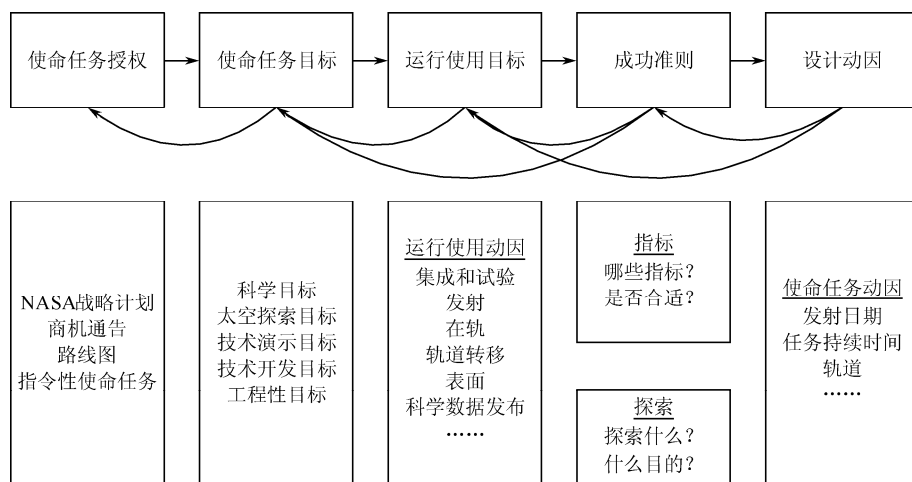


图 4.1-2 利益相关者期望的产品流程

目标定义通过引出利益相关者的需求、能力、外部接口、假设和约束条件来完成。达成一致的目标是一个长期艰巨的过程。在整个系统工程流程中，与利益相关者主动反复交互是使所有参与团队在应该做什么和如何做上达成一致理解的有效途径。弄清谁是主要利益相关者及谁有处置冲突的决策权很重要。

项目团队同样要确认可能会面对的约束条件。约束条件是必须要满足的条件。有时约束条件是由外部因素决定的，如轨道力学因素或技术状态因素，有时约束是由整个预算环境造成的。在确定使命任务目标的同时归档约束条件和相关假设是十分重要的。

运行使用目标也需要包括在利益相关者期望的描述中。运行使用目标确定使命任务中如何运行、使用和操作才能完成使命任务目标。

使命任务和运行使用成功准则描述使命任务必须成功完成的内容。这将表现为对科学试验型使命任务成功的度量和对空间探索型使命任务成功的度量。成功准则同时定义了概念评估和探索活动需要达成的满意程度。成功准则紧扣利益相关者期望，与工程性需求和约束条件共同作用于顶层需求。

设计导向极大地依赖于运行使用构想，包括运行使用环境、轨道和使命任务期限需求。对科学试验使命任务来说，设计导向可能至少包括使命任务启动日期、持续时间和预定轨道。如果考虑可选择不同轨道，则每个轨道需要单独的构想。对探索使命任务来说，为保证探索成功必须考虑目的地、持续时间、运行操作序列及系统技术状态变化、探险活动。

这一步骤的最终结果是发现和描绘出系统的目标，总体上表达系统最终用户的协议和需求。顶层需求和成功准则表示利益相关者意见的产品示例。

4.1.1.3 输出

获取利益相关者期望的典型输出包括如下所述。

- **顶层需求和期望：**这些可能是待开发产品的顶层需求和期望（如需求、期求、能力、约束条件和外部接口）。

- **运行使用构想：**描述系统在全寿命周期各阶段如何运用以满足利益相关者期望。它从使用的角度描述系统的特征且促进对系统目标的理解。例如，运行使用构想文档或使命任务设计参考。

注：在项目所有阶段中都必须有利益相关者参与，这一点极其重要。这种参与应当作为一种自动修正的反馈循环嵌入项目中，以便显著增强使命任务成功的可能。利益相关者的参与可以帮助建立互信，从而作为目标产品和服务确认和验收的基础。

4.1.2 明确利益相关者期望流程指南

运行使用构想是获取利益相关者期望、需求和确定项目结构的重要成分。它是系统中与用户相关联的需求开发和结构开发的出发点。它是此后各类文档（如运行使用计划、发射和早期轨道计划、使用手册等）的开发基础；它同时为长期的使用计划开发活动提供基础，这些活动如运行使用设施、人员安排和网络化进度的安排。

运行使用构想是系统需求中的重要导向，必须在系统设计过程早期予以考虑。通过思考运行使用构想和用例经常能揭示出可能会被忽视的需求和设计功能。证明这一点的简单例子是新添“在使命任务某个特殊的阶段允许通信”的系统需求。这可能需要在专门的位置增加一个天线，而这在既定的使命任务中可能并不需要。

运行使用构想对所有项目同样重要。对科学项目来说，运行使用构想描述系统如何运用才能达到使命任务成功需要的度量指标，这些项目通常由度量指标集中的指标值驱动。对探索项目来说，运行使用构想似乎更加复杂。通常有更多的运用阶段，更多的技术状态变化，以及人类交互需要的额外通信链路。对于载人航天飞行的功能和目标应当在项目早期就要在航天员和系统之间分派清楚。

运行使用构想应考虑包括集成、测试、发射和处置的所有运行使用环节，运行使用构想中包含的典型信息有主要阶段的描述、运行使用时间线、运行使用方案和/或使命任务设计参考、全系统通信策略、指令和数据结构、运行使用设施、综合后勤保障（重复补给、维护和组装）及关键事件。运行使用方案描述系统运用的动态视图并包括系统感知功能的各种模式和模式转换，包括外部接口交互。对于探索使命任务，多个使命任务设计参考组成一个运行使用构想，设计和性能分析要求系统需求必须满足这些使命任务设计参考。图 4.1-3 说明了科学使命任务运行使用构想中包含的典型信息。图 4.1-4 所示的是全系统的运行使用体系架构。更多开发运行使用构想的信息，参见 ANSI/AIAA G-043-1992《运行使用构想文档准备指南》。

运行使用时间线为定义系统技术状态、运行使用活动，以及其他按顺序的相关单元提供基础，以完成每个运行使用阶段的使命任务目标。它描述为完成每个阶段使命任务目标的行动、任务及其他按顺序相关单元。根据项目的类型（科学、探索、军事行动），时间线可能相当复杂。

时间线伴随设计而成熟，它开始时表现为主要事件的简单时序，成熟后展示在所有主要使命任务模式下或系统交付时的分系统运行使用详细描述。图 4.1-5 和图 4.1-6 分别描述探月飞行寿命周期早期的时间线和使命任务设计参考。图 4.1-7 给出一个科学使命寿命周期后期的更加细致、完整的时间线。

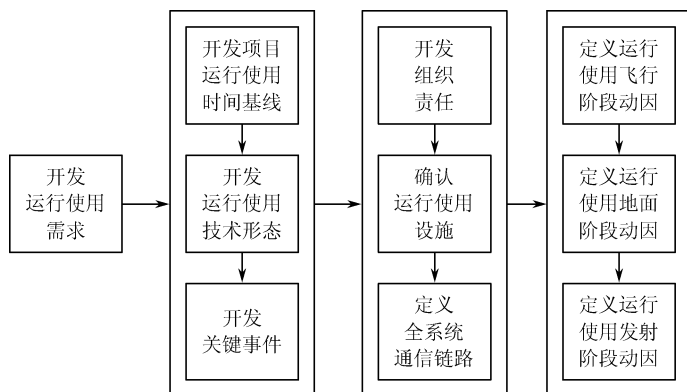


图 4.1-3 科学使命的典型运行使用构想开发

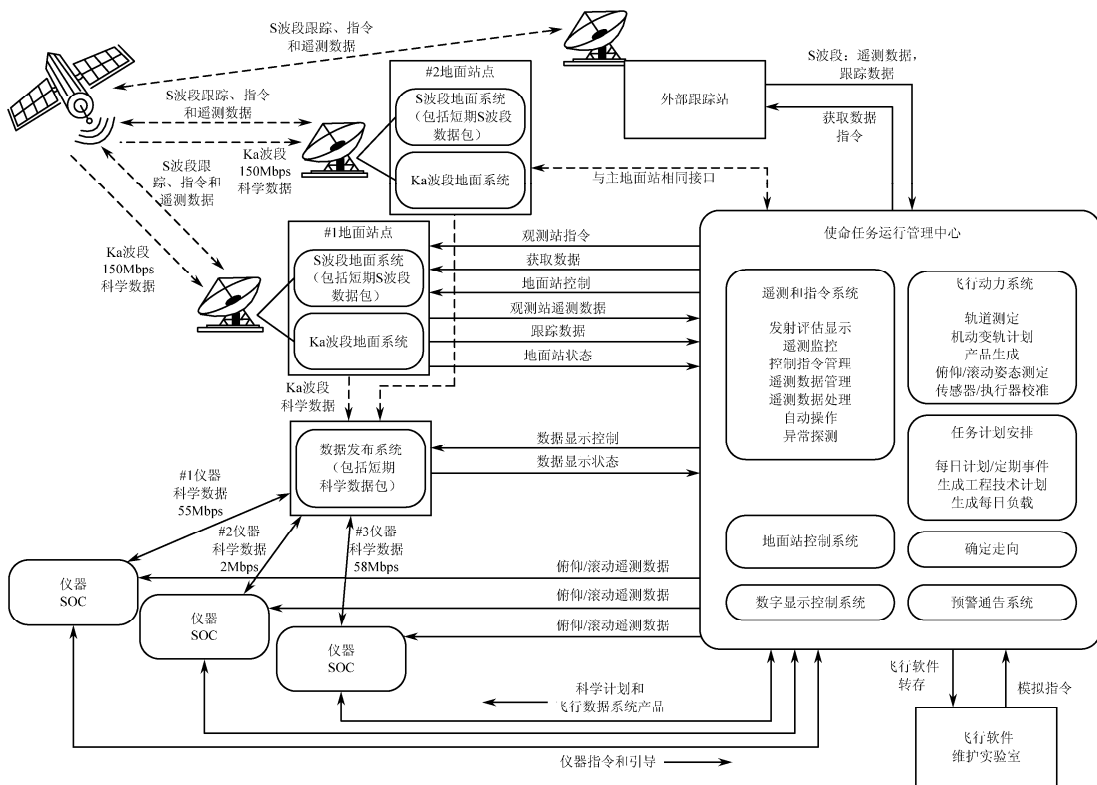


图 4.1-4 全系统的运行使用架构示例

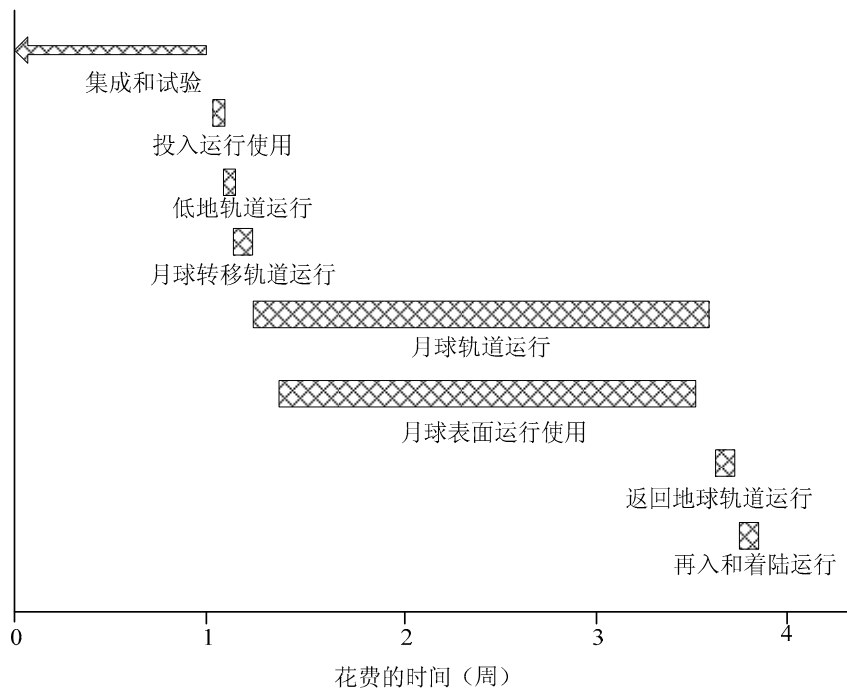


图 4.1-5 寿命周期早期开发的探月飞行时间控制基线示例

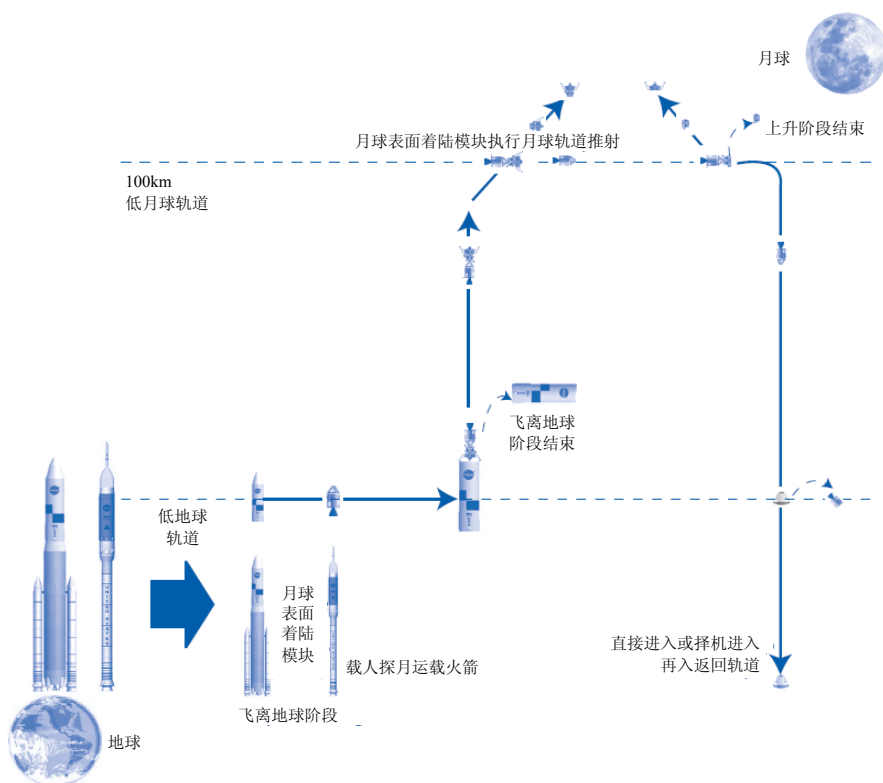


图 4.1-6 寿命周期早期的探月飞行使命任务设计参考示例

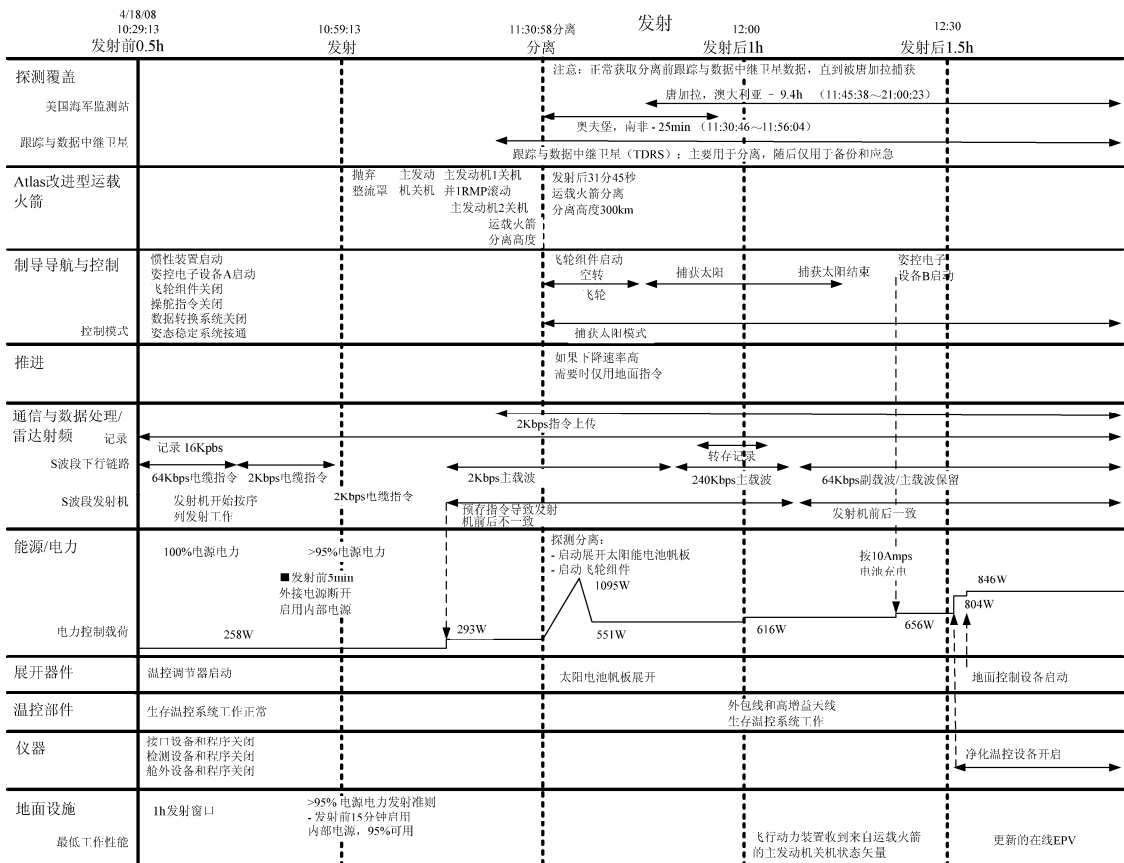


图 4.1-7 科学使命寿命周期后期的更加细致、完整的时间线示例

运行使用构想的一个重要部分是明确运行阶段，它横跨项目阶段 D、阶段 E 和阶段 F。明确运行阶段可为针对完成使命任务目的需要实施的技术状态变更和运行使用活动提供时序结构。每个运行阶段都包括设施、装备和关键事件。表 4.1-1 给出了 NASA 使命任务的典型运行使用阶段的部分通用示例。

表 4.1-1 NASA 使命任务的典型运行使用阶段

运行使用阶段	描 述
集成和试验	项目集成和试验： 在项目集成和试验阶段的后期，在功能试验和环境试验中通过执行运行使用仿真进行系统试验。通过仿真演练全系统命令和数据系统，在项目运行使用想定下提供系统功能和性能的完整验证
	发射集成： 发射集成阶段可能重复进行集成，并在发射集成技术状态下进行运行使用验证和功能验证测试
发射	发射： 发射过程包括发射倒计时、发射升空及在轨推进。在这个阶段里关键事件遥测是重要的导向
	部署： 在轨推进结束后，航天飞行器完成部署并重构其轨道技术状态。典型的关键事件有太阳能电池展开、天线展开和其他部件展开，以及此阶段内发生的轨道修正机动
	在轨校验： 在轨校验用于执行相应系统是否健康的验证。包括准备用于科学实验的飞行系统的在轨定位、校准和参数化
科学运行使用	在轨进行科学实验是飞行寿命周期运行使用的主要部分
安全维护	作为机载故障检测的结果或根据地面命令，航天器可能转换到安全维护模式。该模式被设计成航天器保持在电源保护和热稳定状态，直到故障被排除且科学实验能够恢复

续表

运行使用阶段	描 述
非常规分解和维护	非常规分解和维护可能发生在整个使命任务过程中，可能需要运用既定资源之外的其他资源
退役处置	退役处置发生在项目寿命周期的终点。退役处置或用于提供航天器的坠落控制，或用于航天器转移到废弃轨道的重新定位。对于后一种情况，需要耗尽存储的燃料和电能

4.2 技术需求定义

技术需求定义流程是把利益相关者的期望转换成对问题的定义，然后转换成经认定的技术需求的完备集；这些以“需要”形式陈述的需求能够用于定义产品分解结构模型和相关附属产品的设计方案（产品分解结构模型产品如系统或子系统；相关附属产品如提供或使用数据的外部系统）。需求定义是个递归和反复迭代过程，开发利益相关者需求、产品需求和底层产品/组件需求。需求应该能够描述所有的输入、输出和输入/输出之间的必要关系。需求文档用于组织客户、相关利益者和技术团体需求之间的相互沟通。技术需求定义活动应用于从工程层、项目层、系统层直到底层产品/组件需求文档的技术需求定义。

注：设计团队绝对不能完全依赖接收到的需求进行系统设计和建造，这一点极其重要。与利益相关者不断的反复交流是确保相互之间一致理解每个需求的基础。否则，设计人员可能会因为对需求的不同理解而承担造成误解的风险或设计出非所期望的解决方案。

4.2.1 流程描述

图 4.2-1 给出了技术需求定义流程的典型流图并且标识了表达技术需求定义需要考虑的典型输入、输出和活动。

4.2.1.1 输入

需求定义流程中需要的典型输入应该包括如下所述。

- **顶层需求和期望：**这些是来自客户和利益相关者的关于待开发产品的意见一致的顶层需求和期望（如需求、期求、能力、约束和外部接口）。
- **运行使用构想：**描述系统在寿命周期的各阶段如何运行使用，以满足利益相关者的期望。它从运行使用的视角描述系统特征，并有助于对系统目的的理解。例如，运行使用构想文档或设计任务参考。

4.2.1.2 流程活动

对顶层需求和期望进行初步评估，以理解待解决的技术问题并建立设计边界。通常进行如下活动来建立典型的边界：

- **确定设计方案必须遵从的或系统将使用的约束条件。**在权衡分析时约束条件通常是不能够改变的。

- 辨识已经在设计控制下并且不能变更的那些单元。它有助于缩小对潜在设计方案进行权衡分析的范围。
- 建立系统交互必需的物理接口和功能接口（如机械的、电子的、热学的、人因的等）。
- 为运行使用构想中辨识的系统预期使用范围定义功能和行为期望。运行使用构想描述系统如何运行使用和可能的用例想定。

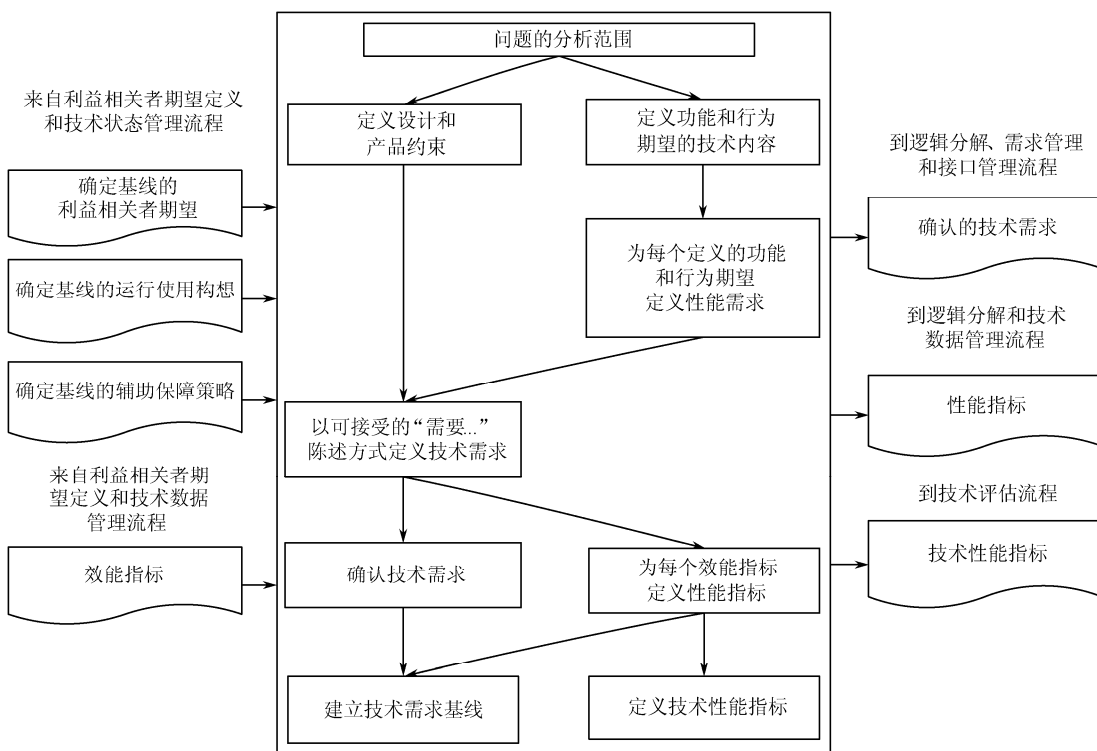


图 4.2-1 技术需求定义流程

随着对约束条件、物理/功能接口和功能/行为期望的全面理解，需求可通过建立性能标准做进一步定义。性能表述为需求的定量部分，用来表示每个产品被期望完成的功能。

最后，需求应该被定义为可接受的“需要”阐述，每个阐述仅含一个“需要”的完整语句。参见附录 C《如何写好需求的指南》和附录 E《如何确认需求》。良好的需求文档可以为利益相关者和技术团队双方带来特定的益处，见表 4.2-1。

表 4.2-1 良好需求写作的益处

益 处	理 由
为利益相关者和开发者就产品用于做什么的问题达成一致建立基础	产品需求中指定的待实现功能的完整描述有助于潜在用户决定该产品是否满足了他们的要求或产品必须如何改进才能满足他们的需要。在系统设计过程中，需求分配到分系统（如硬件、软件及其他主要的系统组件）、人或流程中
降低开发成本，因为减少了为说明低水平、有缺失和难懂的需求描述而做的重复工作	技术需求定义流程的活动促使利益相关者在设计开始之前更加严格地考虑所有需求。对需求的细致评审可以在开发周期的早期揭示出遗漏、误解和不一致，此时这些问题较容易解决，从而降低在寿命周期后续阶段中重新设计、重新制造、重新编码和重新试验的成本

续表

益 处	理 由
为预估成本和进度提供基础	需求中给出的待开发产品描述是估计项目成本的现实基础，也可用于对报价或价格估算进行评价
为验证和确认提供控制基线	根据一个好的需求文档，相关组织可以更有效地开发其验证和确认计划。系统和分系统的试验计划和程序都要通过需求生成。作为开发的一部分，需求文档为此提供控制基线，基于此度量对需求的遵从度。需求还用于为利益相关者提供系统验收的基础
便于交付	需求使产品向新用户交付或用于构建新机器更加容易。利益相关者将发现产品转交到组织内其他部分更加容易，开发者将发现向新的利益相关者转交产品或重用产品更加容易
为进一步提升打下基础	对于已完成的产品，需求为其今后可能的提升或改造打下基础

4.2.1.3 输出

技术需求定义流程典型的输出应包括如下所述。

- **技术需求：**这是被认可的表示待解决问题完整描述的需求集，以及客户和利益相关者确认和认可的其他需求。对获取的需求进行归档，例如，系统需求文档、接口需求文档等。
- **技术指标：**基于需求和期望建立的度量指标集，通过跟踪和评估决定整个系统或产品的效能及客户满意度。常用的技术指标有效能指标、性能指标和技术性能指标。参见 6.7 节的进一步详细叙述。

4.2.2 技术需求定义指南

4.2.2.1 需求类型

项目需求的完备集包括功能需求（需要执行什么功能）、性能需求（这些功能必须执行到何种程度）和接口需求（所设计单元的接口需求）。对于空间项目，这些需求依照产品分解结构分配到设计单元中。

功能需求、性能需求和接口需求非常重要但并不构成项目成功必需的需求集全部。空间部段设计单元必须在项目环境中生存并持续工作，这些环境影响可能包括辐射、热学、声学、机械载荷、污染、微波辐射频率及其他。此外，可靠性需求将影响在设计健壮性、故障容错性和冗余方面的设计选择。安全性需求将影响在提供各类功能冗余方面的设计选择。其他专业特性的需求可能同样影响设计选择，包括可生产性、可维护性、可用性、可升级性和人的因素等。不同于将功能需求分解或分配到设计单元，上述需求通过主要的项目相关单元征集。为满足这些需求，设计活动需要对设计方案进行细致的分析。图 4.2-2 显示了功能、运行使用、可靠性、安全性和特性需求的特征。顶层使命任务需求产生于使命目标、工程上的约束和假设，这些通常聚合到包含图 4.2-2 所示需求分类的功能和性能需求中。

1. 功能需求

对于产品全寿命周期中所有预期的应用，需要指定其功能需求。功能分析用于获取功能和性能的需求。基于建立的标准（如相似的功能、性能或其组合等），需求被划分为组，以便

于需求分析聚焦。功能需求和性能需求分配到功能分组和子级功能、目标、人员和流程，此时需考虑受时间影响的功能顺序。采用输入、输出和接口需求形式自顶向下辨识和描述每项功能，以便能够在更大的功能组合中识别分解的功能。功能按照逻辑顺序分配，因此，系统任何指定的运用能够通过全系统路径追踪，反映系统必须实现的所有功能的顺序关系。

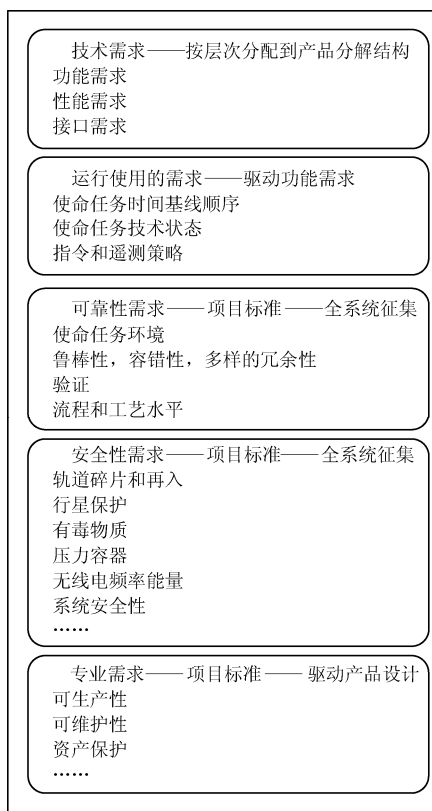


图 4.2-2 功能性的、运行使用的、可靠性的、安全性的和专业性的需求特征

询问如下类型的问题有助于形成运行使用构想和想定：需要执行什么功能？这些功能需要在何处？在什么运行使用和环境条件下执行及是否经常执行等？通过思考这些问题经常揭示出额外的功能需求。

注：功能需求是定义为实现系统目标需要做到什么功能。性能需求是定义系统功能需要执行到何种程度。

2. 性能需求

性能需求量化定义系统需要执行功能的程度。同样，通过询问如下类型的问题有助于形成运行使用构想和想定，并描绘出性能需求：多少频度和多大程度？需要什么精度（如需要怎样精确的度量指标）？形成什么定性和定量的输出？在什么强度（如最大同时数据请求）或环境条件下，需要多少持续时间？在什么取值范围内，有多少偏差许可？在多少最大通量和带宽容量内？

功能和性能需求示例

初始功能陈述

推力矢量控制器需要能够控制飞行器俯仰和偏航方向。

该陈述描述推力矢量控制器必须执行的高层功能。技术团队需要将该陈述转换为面向设计的功能和性能需求。

功能需求及相应的性能需求

- 推力矢量控制器需要能够以最大角度 $(9 \pm 0.1)^\circ$ 万向转动引擎。
- 推力矢量控制器需要能够以最大角速率 $(5 \pm 0.3)^\circ/\text{s}$ 万向转动引擎。
- 推力矢量控制器需要能够提供 $(40\,000 \pm 500)$ 磅 (1 磅=0.4536 千克) 动力。
- 推力矢量控制器需要具有 $(20 \pm 0.1)\text{Hz}$ 响应频率。

在可能的情况下，使用如下方式定义性能需求：

- (1) 阈值（系统执行使命任务需要的最小可接受值）。
- (2) 性能需要的控制基线水平。

通过阈值和控制基线的需求指定性能，可以为系统设计人员提供研究考察不同设计方案的权衡空间。

所有定性的性能期望必须进行分析并转换为定量的性能需求。权衡研究通常可以帮助量化性能需求。例如，权衡可以显示性能需求的微小放松是否会产生系统费用显著下降，或稍多的资源是否会产生更显著有效的系统。临界值和目标值的逻辑依据应当与需求同时记录，以便在性能需求必须变更时能够理解当时提出该需求的原因和初衷。通过权衡分析量化或改变的性能需求必须标识。关于权衡分析的更详细信息，参见 6.8 节的决策分析。

注：性能需求不要制定得过于严格。例如，对于必须能够使用充电电池运行的系统，如果性能需求指定充电时间需要少于 3h，而 12h 的充电时间已经足够，则潜在的解决方案将可能被排斥。同样，如果性能需求指定质量必须在 $\pm 0.5\text{kg}$ 以内，而 $\pm 2.5\text{kg}$ 已经足够，这样可能导致产品未增加价值而费用却大幅增长。

3. 接口需求

为系统包括附属系统定义所有的接口需求十分重要。外部接口组成沟通产品和周边世界的边界。接口类型包括操作命令和控制指令、计算机之间、机械的、电子的、热学的和数据的接口。定义接口的一个有用工具就是相关背景图（参见附录 F），它描述产品及其所有外部接口。一旦产品组件被定义，框图显示待开发系统的主要组件、组件间互连和外部接口，用于定义组件和组件之间交互。

与产品整个寿命周期所有阶段关联的接口应当考虑，例如，与试验环境、运输系统、综合后勤保障系统、制造设备、操作人员、用户和维护人员的接口。

完成技术需求定义后，需要重新审视接口图，并且精确改进已记录的接口需求，以包含新辨识需求的内部和外部接口的需求信息。关于接口的更多信息参见 6.3 节。

4. 环境需求

每个空间使命任务都有独自的环境需求，并应用于飞行阶段的单元。辨识特定使命任务的外在和内在环境、分析和量化预期的环境、针对预期环境开发设计指南并建立相应价值体系是系统工程的关键功能。

环境包络线应该考虑在地面试验、存储、运输、发射、部署，以及寿命周期内的常规运行使用所能遭遇到的所有状况。从使命任务环境派生出的需求应该包括在系统需求里。

必须说明的是，相关外部和内部环境包括加速度、振动、震动、静态负载、声环境、热环境、污染、乘员引发的负载、辐射的总剂量/辐射影响、单一事件影响、表面和内部电荷、轨道碎片、大气的（氧原子）控制和性质、姿态控制系统扰动（大气阻力、重力梯度、太阳压强）、磁场的、发射时压力梯度、微生物的生长、地面和在轨微波辐射频率。

需求结构必须说明应用于项目各单元使命任务环境的专门工程领域。这些学科领域将系统单元需求集中在电磁干扰和电磁兼容性、接地、辐射和其他屏蔽、污染保护和可靠性等方面。

5. 可靠性需求

可靠性可以定义为一个设备、产品或系统在特定的运行使用条件下在给定的时间内不出现故障的概率。可靠性是系统固有的设计特征，作为在使用和保障成本及系统效能方面的主要影响因素，可靠性在确定系统费效关系中起关键作用。

可靠性工程是一个重要的专业学科，影响达成有效系统的目标。可靠性工程主要在系统工程过程中完成，通过主动设计实现特定的特征，并为设计权衡、试验计划、运行使用和综合后勤保障计划的系统可靠性做独立的预测，确保系统在整个使命任务过程中能在预计的物理环境中运行使用。

可靠性需求确保系统（分系统如软件和硬件）能像整个使命任务过程中期望的那样在预计的环境和条件下运行使用，并确保系统有能力经受住一定数量和类型的错误、误差或故障（如经受住振动、预期的数据率、命令和/或数据错误、单事件扰动和温度变化达到设定的极限等）。环境可能包括地面（运输和控制）、发射、在轨（地球轨道或其他轨道）、行星式飞行、再入和着陆；也可能包括某种模式软件的环境或运行使用状态。可靠性强调设计和验证需求，以满足运行使用要求的水平，并满足对所有预期环境和条件下的错误和/或故障容错水平。可靠性需求覆盖了错误/故障的预防、检测、隔离及恢复。

6. 安全性需求

NASA 广泛使用的“安全性”术语包含了人员（公众和职工）、环境及资产的安全性。安全性需求有两类——确定性的和风险性的。确定类安全性需求是行动或性能阈值的定性或定量定义，与使命任务相关的设计、系统或相应活动必须满足这个阈值要求，以保证这些设计、系统或活动是安全的。确定类安全性需求例子有安全设备的结合（如在系统中使用防止液压升降饥/液压臂的延伸超过预设安全高度和长度极限的物理栓件）；系统输入变量允许取值的限制范围；在系统某种运行模式或状态下，输入命令限制检查以确保它们在指定的安全限制或约束内（如飞机只有在空中飞行状态下，收缩起落装置的命令才是被许可的）。对那些标识为“安全关键”的组件，需求包括功能冗余或故障容错，以允许系统在出现一个或多个故障时仍满足需求或简化系统功能性要求保证其处于安全状态（如双冗余的计算机处理器，安全状态处理器备份）；如果某些特定值（如温度）超过指定安全极限，能够探测并自动关闭系统；仅使用经过批准的特定计算机语言编写的安全关键性软件的内部模块；警示或报警装置及安全性流程。风险类安全性需求是在考虑与安全性相关的技术性能指标及其相应不确定性的基础上建立的，至少是部分建立的需求。风险类安全性需求的例子如在确定置信水平下乘员损

失概率 ($P(LOC)$) 不超过设定值 “ p ”。满足安全性需求需要辨别和排除危险,降低危险带来事故发生的可能性,或在可接受水平上降低危险及其引发相应事故的影响(更多关于安全性内容参见 NPR 8705.2 《空间系统的人员级别需求》、NPR 8715.3 《NASA 通用安全性工程需求》、NASA-STD-8719.13 《软件安全性标准》)。

4.2.2.2 人因工程需求

在载人空间飞行中,人员作为操作者和维护者,是使命任务和系统设计中的关键组成部分。人的能力和局限必须以材料特性和电子组件特征同样的方式在设计中予以考虑。人因工程是研究系统与人之间接口及交互的学科,它提出需求、标准和指南以确保整个系统能够具备所设计的功能,为人员提供有效空间。

人员最初通过使命任务整体分析集成在系统中。像使命任务功能被分配到系统结构、技术能力、成本因素和员工能力那样,使命任务功能被恰当地分配给操作人员。一旦完成功能分配,人因工程分析者与系统设计者共同工作,确保能够为操作人员和维护人员提供设备、工具和接口,使其安全有效地执行所安排的工作。

NASA-STD-3001 《NASA 空间飞行人员系统标准(卷 1): 乘员健康》要求保证对乘员来说系统是安全和有效的。该标准关注的是与系统集成在一起的人员、确保人员保持健康和有生命力的度量指标(休息、营养、医疗护理、锻炼等)、工作场所环境、乘员与系统物理接口和认知接口。

4.2.2.3 需求分解、分配和确认

需求按系统层次结构进行分解,顶层需求来自总统指示、使命任务主管、工程项目、NASA 总局、客户和其他利益相关者。这些顶层需求都被划分为功能需求和性能需求,并在系统内进行分配。随后进一步在单元和子系统中进行分解和分配。这个分解和分配过程持续进行直到完成完整的满足需求的设计。在每一层次的分解中,全部派生需求在进入下一层分解之前必须通过根据利益相关者期望或较高层次需求进行的确认。

需求直到最底层的可追溯性确保每个需求都是满足利益相关者期望所必需的。需求没能被分配到更低层次或未能在更低层次实现,将导致设计不能够满足目标而成为无效设计。反过来,低层次需求不能被上层需求追溯将导致无法证明的超标设计。层次分解流程如图 4.2-3 所示。

图 4.2-4 所示的是典型科学使命下科学要点的需求自顶向下成功分解和分配的例子。理解和记录需求之间的关系非常重要,这会降低误解的可能性、出现不满意设计的可能性和相关成本增加的可能性。

从阶段 A 到阶段 B,将会出现需求和约束的变更。所有的变更都必须进行评估以确定其对上一层次和下一层次需求的影响,同样,所有变更也要服从评审和正式审批环节,作为正式变更控制流程的一部分来维护可追溯性和确保任何变更的影响都针对系统所有部分做完整评估。如果使命任务巨大且牵涉多个中心或横跨其他组织和机构,就需要更加正式地变更控制过程。

4.2.2.4 获取需求和需求数据库

在编写需求的时候,获取需求陈述,以及获取与每个需求相关联的元数据是很重要的。元数据是阐明和连接需求的必要支撑信息。

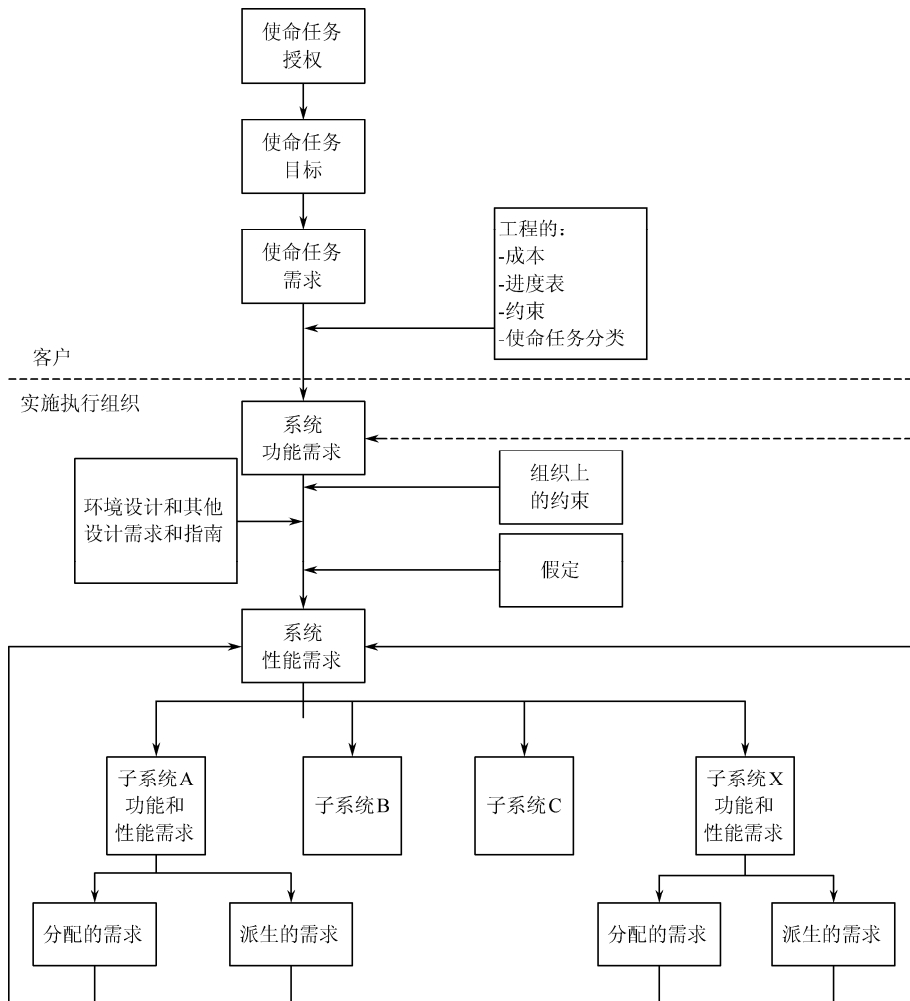


图 4.2-3 层次分解流程

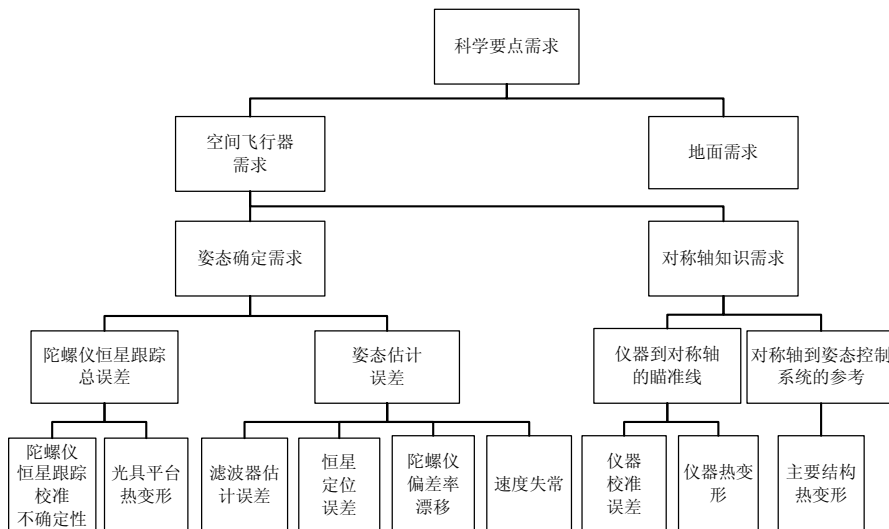


图 4.2-4 科学要点需求的分配和流程

针对每个开发的需求，相应的验证方法必须要考虑周到。验证方法包括试验、检查、分析和演示。确保指定验证方法时未覆盖的那些新的和派生的需求已经归档。例如，在集成和试验时需要附加测试端口，为内部信号增添可视性。如果需求不能被验证，那么它不适合作为需求或需要重写需求陈述。例如，“最小化噪声”需求就是模糊的，不能被验证。如果需求重新陈述为“组件 X 的噪声水平应该在 Y 分贝以下”，它就能被清楚地验证。元数据类型实例见表 4.2-2。

表 4.2-2 需求元数据类型

项 目	功 能
需求 ID	需求 ID 为排序和跟踪提供唯一的编号系统
依据	在编写需求时为阐明其意图提供附加信息（参见“依据”注记）
追溯	在父层需求和较低层次（派生）的需求间获得双向可追溯性，并获取需求之间的关系
所有者	负责编写、管理和/或批准需求变更的个人或团体
验证方法	获取验证的方法（试验、检查、分析、演示），应当在需求开发时确定
验证领导	被指派负责需求验证的个人或团体
验证层次	为待验证的需求指定层次（如系统层、分系统层、单元层）

需求数据库对获取需求和相关的元数据来说是个非常有用的工具，且对展现需求间的双向可追溯性也十分有用。数据库随时更新变化，可用于追踪与需求相关的状态信息，如待决策状态/待解决状态、解决方案日期和验证状态。每个项目应该决定获取什么元数据。数据库通常处于中心位置，这样便于整个项目团队使用（需求验证矩阵样本见附录 D）。

依 据

依据应当包含以下信息并，一直保留。

- **需求的理由：**通常需求的理由不清晰，在形成需求文档的过程中若不记录则可能丢失。理由可能指向一个约束或运行使用构想。如果存在清晰的上层需求或能够解释理由的权衡研究结果，可以作为参照。
- **归档假设：**如果在记录需求时假设技术开发已经完成或假设技术使命任务成功完成，则需归档此假设。
- **归档关系：**与产品期望运行使用的关系（如对利益相关者如何使用此产品的期望）。该项工作与运行使用构想相关。
- **归档设计约束：**在进行设计时，由决策过程带来的约束。如果需求陈述了实施的方法，则依据“需要”形式陈述为什么确定将解决方案限制在此实施方法的决策。

4.2.2.5 技术标准

1. 标准应用的重要性

标准为工程和项目建立公共技术需求提供可信的基础，避免需求不兼容并确保至少满足最低程度的需求。公共标准还能降低运行成本、检查成本及供货成本等。标准（规范）应用于产品全寿命周期以建立设计需求和边界、材料和工艺规范、测试方法和接口规范。标准作为需求（或指南）应用在设计、制造、确认、验证、接收、使用和维护中。

2. 标准选择

NASA 技术标准政策在 NPD 8070.6《技术标准》中提供，说明标准的选取、剪裁、运用和控制。总体上看，在 NASA 工程和项目标准中权限的顺序如下：

- 法律规定的标准（如环境标准）；
- 国家或国际工业界共同认可的通用标准；
- 其他的政府标准；
- NASA 政策指南；
- NASA 技术标准。

NASA 也可指定限定的或“核心的”标准，所有工程在技术可行的情况下必须应用这些标准。放弃制定核心标准必须得到 NASA 总局的审议和许可，除非另作指定。

4.3 逻辑分解

逻辑分解是生成详细功能需求的过程，使 NASA 工程和项目能够实现满足相关利益者期望。这个流程确定系统在每个层次上必须要完成“什么”才能实现项目成功。逻辑分解利用功能分析来构造系统结构，分解顶层（上层）需求，并把它们向下分配直到所需的项目最底层。

逻辑分解流程用于如下方面：

- 增强对定义的技术需求和需求间关系的理解（如功能的、行为的和时间的需求）。
- 为了得到设计方案定义流程的输入，将上层需求分解为一组逻辑分解模型及其相关的一组派生技术需求。

4.3.1 流程描述

图 4.3-1 所示的是逻辑分解流程的典型流程图，给出了在逻辑分解中需考虑的典型输入、输出和活动。

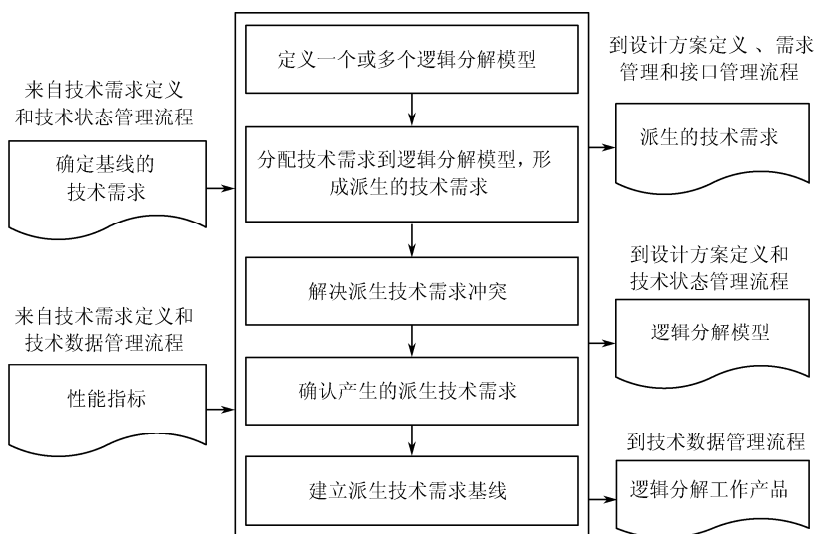


图 4.3-1 逻辑分解流程

4.3.1.1 输入

逻辑分解流程中需要的典型输入如下所述。

- **技术需求：**一组经确认的需求，代表着待解决问题的描述，其通过功能分析和性能分析建立，并得到客户和其他利益相关者的批准。获取的需求应归档，如系统需求文档，产品需求文档和接口需求文档。
- **技术指标：**基于期望和需求建立起来的指标集将被跟踪和评估，以决定整个系统或产品的有效性及客户满意度。这些指标包括效能指标和性能指标，以及称为技术性能指标的特别子集。进一步信息参见 6.7.2.2 节。

4.3.1.2 流程活动

逻辑分解流程的关键第一步是建立系统架构模型。系统架构定义了硬件、软件、通信、运行等底层结构及关联关系，提供给 NASA、使命任务主管、工程、项目及更低的各个需求层次开展工作。系统架构的建立驱动系统单元和需求向低层功能和需求的分解，直到设计工作能够完成。分解后的子系统、单元间的接口和关系也同时被定义。

一旦建立了顶层（父层）的功能需求和约束，系统设计人员就可以应用功能分析开始规划概念上的系统架构。系统架构可以视为系统功能单元的战略组织，使单元间的作用、关系、依赖性和接口能够清晰的定义和理解。系统架构在战略层面注重系统整个结构和各单元之间配合对整体的贡献，而不是各个单元自身的独立工作。系统开发时，各个单元在确保它们有效地共同工作以达到顶层（父层）需求的情况下，是相互独立开发的。

同功能分解的其他单元很相像，开发一个好的系统层次架构是一个创造性的、递归的和迭代的过程，能达到对项目最终目标和约束条件的最佳理解，同样能达到对实现目标产品交付的潜在技术方法的良好认识。

关注项目的最终的顶层需求（或父需求）及约束条件，系统结构设计人员必须至少开发一个、最好是多个能完成工程目标的系统概念架构。

每个概念架构都包含功能单元的规范（单元做什么）、它们的相互关系（接口定义），以及运行使用构想，即从运行使用开始到使命任务结束分布在不同位置和环境的各个部段、子系统、单元、元件等如何作为整体系统运行使用。

概念架构的开发过程必须是递归和迭代的，要从利益相关者和外部评审者那里得到反馈，同样也要从子系统设计者和使用者那里得到反馈，这些反馈应当尽可能多，以增加完成工程最终目标的可能性，同时减少成本和进度超出的可能性。

在使命任务的早期，多个概念架构被开发。成本和进度表约束条件将最终限制工程或项目能够维护多个概念架构的时间长短。对所有的 NASA 工程，架构设计须在论证阶段完成。多数的 NASA 项目及紧密联系的工程，单独的架构选择发生在阶段 A，架构和运行使用构想将在阶段 B 确立控制基线。高层架构偶尔会因向低层的分解产生设计、成本或进度方面复杂性而需要变更。

除架构设计师的创造性思想外，还有多个工具可运用于系统架构的开发。这些主要是建模和仿真工具、功能分析工具、结构框架和权衡研究（如采用国防部体系架构框架（DODAF）的方法构建系统架构，见注记）。随着每个概念的开发，架构分析模型、其组件和组件的运用也会随着项目的进展而更加逼真地开发。功能分解、需求开发和权衡研究也随后进行。随着需求的分解和设计的成熟，这些活动将多重迭代并反馈到演化的架构概念中去。

功能分析是用于系统架构开发和功能需求分解的主要方法。它是确定、描述和关联系统必须执行的功能，以满足系统目标的系统化过程。功能分析确定和连接系统功能、权衡研究、接口特征和需求原理。这些通常都基于反映系统利益所在的运行使用构想。

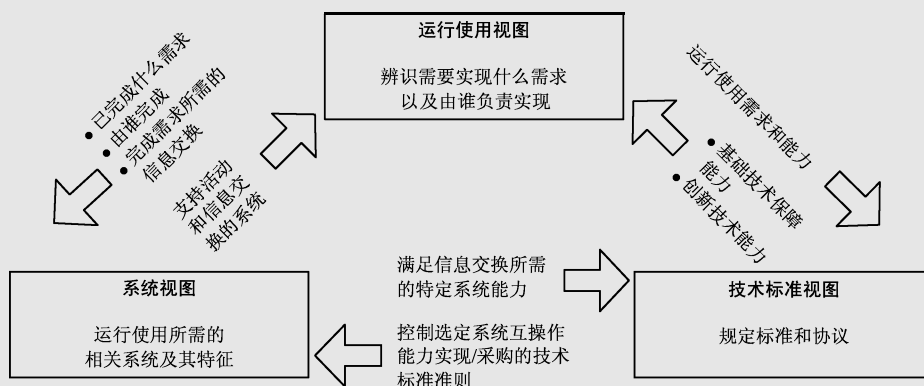
执行功能分析三个关键步骤如下：

- 把顶层需求转化为必须完成以实现需求的功能。
- 分解和分派功能到产品分解结构的更低层。
- 确定和描述功能接口和子系统接口。

DOD 架构框架（DODAF）

在过去十年中，架构框架技术的进步使之成为用于对演化的复杂体系进行描述和特征化的新方法。在此氛围下架构描述非常有用，可用于确保利益相关者的需求被清晰理解和排序，确保优先考虑关键细节（如互操作性），确保主要投资决策基于战略性考虑。认识到这一点，美国国防部确立了在投资规划、采办和联合能力集成方面指定使用 DODAF 的政策。

架构可以理解为“组件的结构及其相互关系，以及全程控制其设计与演化的原则和指南。”^①为了描述架构，DODAF 定义了若干视图：运行使用视图、系统视图和技术标准视图。此外，还包括字典和概要信息（见下图）。



在每一个视图中，DODAF 包含特定的产品。例如，在运行使用视图中，包含运行使用节点的描述、它们的关联性，以及信息交换需求。在系统视图中，包含所有运行使用节点和相互关联构成的系统描述。并非所有 DODAF 产品都与 NASA 系统工程相关，但它的基础概念和形式体系可以用于技术需求定义和决策分析流程的复杂问题结构描述。

基于美国电气与电子工程师学会（IEEE）的 STD 610.12 标准定义。

这个流程包括分析每个系统需求以确定为满足需求必须实现的所有功能。每个确定的功能用输入、输出和接口需求描述。这个流程自顶向下重复，因而子功能可以看做更大的功能区域的一部分。功能按逻辑顺序安排，所以，系统任何特定的运行使用都能通过全系统路径追溯。

这个过程是迭代和递归的，并一直持续到系统/架构所有必要的层次完成分析、定义和设定控制基线。功能分解几乎一定有可替换的方式，所以，分解结果高度地依赖于工程师进行分析时的创造性、能力和经验。随着分析进入架构和系统较低层，且系统已被更好地理解，系统工程师必须保持开放的思想信念，回顾和修改以前建立的架构和系统需求。这些变更又必须再次通过架构和系统分解下去，持续的递归过程直到系统被完整的定义，所有需求都被理解且认知为是可行的、可验证的和内在一致的。只有做到这样，系统架构和需求的控制基线方能确定。

4.3.1.3 输出

逻辑分解流程中的典型输出如下所述。

- **系统架构模型：**定义系统各组件（如硬件、软件、通信、使用等）之间的基础结构和关系，定义将需求分解到设计工作能够完成的较低层级的基础。

- **目标产品需求：**定义能使设计方案完成的生产需求、购买需求、编码需求及其他方面需求。

4.3.2 逻辑分解指南

4.3.2.1 产品分解结构

通过产品分解结构和工作分解结构表述的分解形成关于所需产品系统的重要视图。工作分解结构是对完成项目需要开展工作的层次分解。关于工作分解结构开发的进一步信息请参见 6.1.2.1 节。工作分解结构包括产品分解结构，产品分解结构是关于产品如硬件、软件、信息项（文档、数据库等）的层次分解。产品分解结构运用于逻辑分解和功能分析流程中。产品分解结构要展开到最底层，并且有相应的工程师和管理者。图 4.3-2 所示的是产品分解结构的一个示例。

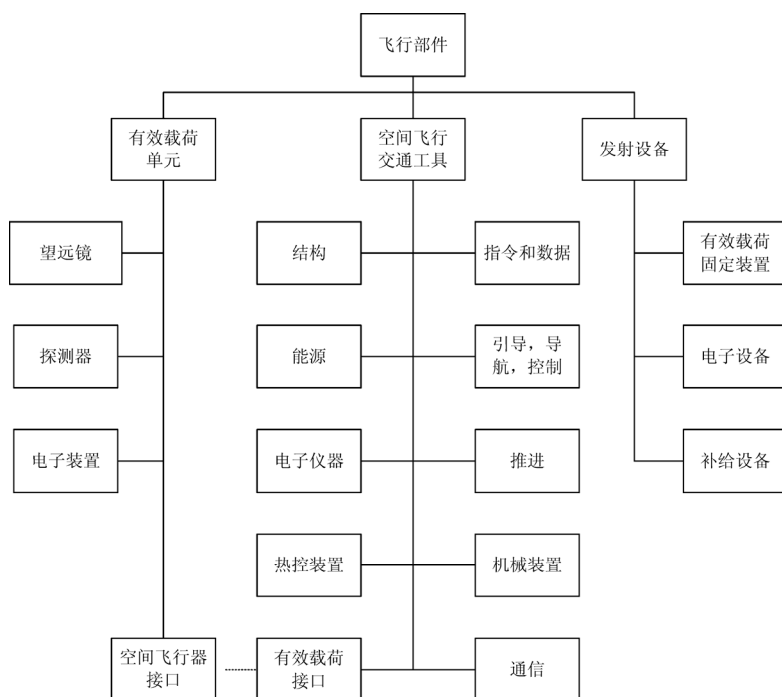


图 4.3-2 产品分解结构示例

4.3.2.2 功能分析技术

尽管有很多技术可用于进行功能分析，一些更常用的方法如下：

- (1) 功能流框图，用来描述任务的顺序和关系；
- (2) N2 图（或 $N \times N$ 交互矩阵），用来从系统的观点确认主要因素间交互关系或接口；
- (3) 时间线分析，用于描述有时间限制功能的时间顺序。

1. 功能流框图

主要的功能分析技术是功能流框图。功能流框图的目的是显示系统必须完成的所有功能的顺序关系。当功能流框图完成后，这些图展示完整的活动网络，引导系统功能的实现。

功能流框图专门描述紧随前一事件的每个功能事件（通过模块进行描述）。有些功能可以并行实现或采取其他路径实现。功能流框图网络显示了必须发生的事件的逻辑顺序，它不能够描述功能持续时间或功能间隔时间。功能持续时间和功能间隔时间可能在一秒到数周的范围内容变化。需要使用时间线分析理解有时间限制的需求（参见本小节关于时间线分析的讨论）。

功能流框图是功能导向的，不是设备导向的。换句话说，它们确认什么必须发生而绝不回答功能是如何实现的。在给定的层次上，每个模块的“如何”通过定义为实现该模块下更低层次需要的功能来描述。这样，在系统各个层次上，功能流框图通过更高层次单个使命任务在功能分解中确定为低层任务，自顶向下开发。功能流框图在每个层次展示所有使命任务的逻辑和顺序关系，以及它们需要的输入和预期输出（包括可能的指标），还有与更高层单一使命任务的清晰联系。

图 4.3-3 给出了功能流框图的一个例子。该功能流框图描述空间飞行器的完整飞行使命任务。图中第一层的每个模块都可扩展为第二层图中的一系列功能，如“执行使命任务”。注意：图中同时显示了输入（转移到 OPS 轨道）和输出（转移到 STS 轨道），用于初始化接口标识和控制过程。图的第二层中每个模块可进一步开发为一系列功能，如图中第三层所示。

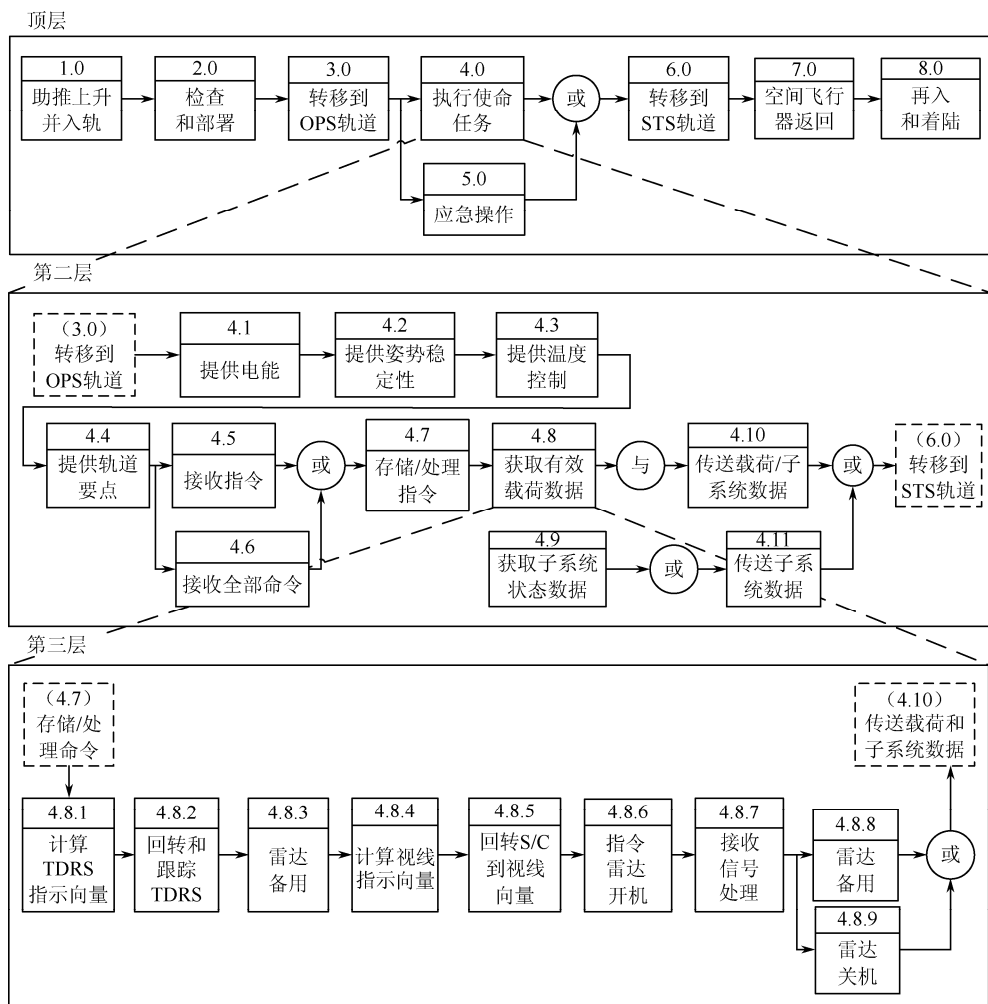


图 4.3-3 功能流框图示例

功能流框图通过确定实现每个功能的各种方法，用于开发、分析及分解需求，同样用于确认有益的权衡研究。在某些情况下，可选择不同的功能流框图表示满足特殊功能的多种方法，直到获得能够在各种方案中选择的权衡研究数据。流程图同样提供对系统总体运行使用的理解，作为开发运行使用和意外处置规程的基础，并定位那些变更运行使用规程则能简化整个系统运行使用的关键区域。

2. N2 图

N 平方图（ N^2 图或 N2 图）用于开发系统接口。图 4.3-4 所示的是 N2 图的一个例子。系统组件或功能放置在对角线上； $N \times N$ 矩阵方形的余项代表接口输入和输出。出现空白的地方表示相应组件和功能间没有接口。N2 图能连续拆解到较低层次直到组件功能层。除定义接口之外，N2 图还能确定接口间可能出现冲突的区域，且突出表示输入和输出依赖性的假设和需求。

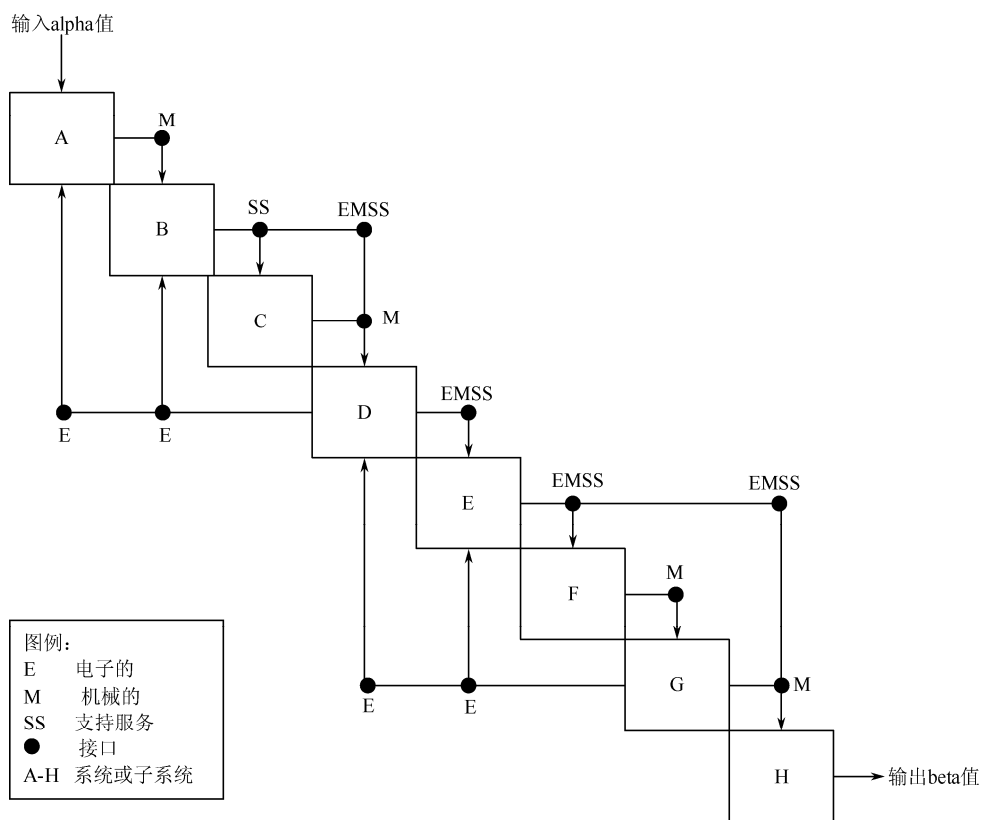


图 4.3-4 N2 图示例

3. 时间线分析

时间线分析增加了对功能持续时间的考虑，在时间对使命任务的成功性、安全性、资源利用率、最短停工期和/或提升可用性十分关键的领域使用。时间线分析能运用于如空间飞行器指令排序和发布，而对那些时间不是关键因素的功能序列，功能流框图或 N2 图已经足够。经常归类于有时间限制的领域如下：

- 功能影响系统反应时间；
- 使命任务转换时间；

- 倒计时活动；
- 需利用设备和人员达到的最佳功能依赖于特殊活动的时间。

时间线表格用于实施和记录时间关键功能和功能序列的分析。对于有时间限制的功能序列，时间需求指定相关的容错度。附加工具如数学模型和计算机仿真对建立每个时间线的持续时间也许是必要的。

关于功能框图、N2 图、时间线分析和其他功能分析方法的信息，参见附录 F。

4.4 设计方案定义

设计方案定义流程用于把来自利益相关者期望的高层需求和逻辑分解流程的输出转化为设计方案。这牵涉到把定义好的逻辑分解模型及其相应派生的技术需求转换为备选方案。通过详细的权衡研究对这些备选方案进行分析，从而得出适当的方案选择。

选定的备选方案被完整定义为一个满足技术需求的最终设计方案。设计方案定义将用于生成目标产品规范，用于生产产品和进行产品验证。根据目标产品是否有需要定义的附加子系统，设计方案定义流程可能需要进一步改进。

4.4.1 流程描述

图 4.4-1 给出设计方案定义流程的典型流程框图，且给出在设计方案定义中需考虑的典型输入、输出和活动。

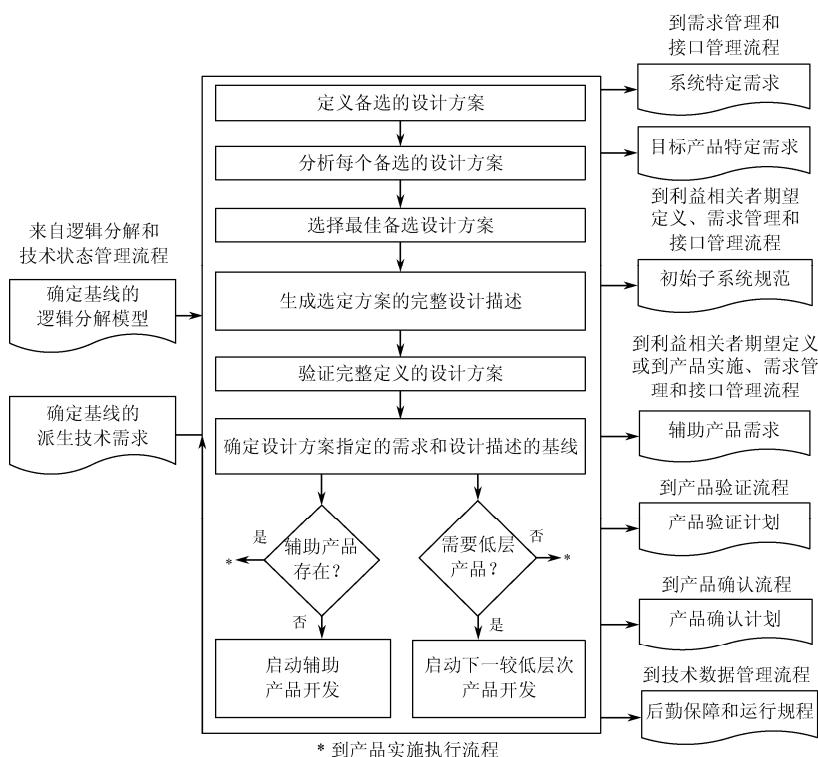


图 4.4-1 设计方案定义流程

4.4.1.1 输入

设计方案定义流程开始时需要的一些基本的输入如下所述。

- **技术需求：**客户和利益相关者的需要，该需要转化为合理的经过确认的完整的系统需求，包括所有接口需求。
- **逻辑分解模型：**用一个或多个方法分解的需求（如功能、时间、行为、数据流、状态、模式、系统架构等）。

4.4.1.2 流程活动

1. 定义可选的设计方案

系统在其整个寿命周期内的实现，牵涉到一系列备选行动方案的决策。如果备选方案能被精确地定义并在成本—效能空间上分别被完全理解，那么系统工程师将能自信地在其中做出选择。

为了得到足够可信的便于良好决策的评估，通常需要对可能的设计空间进行更深入的研究，如图 4.2-2 所示。然而应该认识到，这个图表述的既不是项目寿命周期（包含从概念开发到退役处置的系统开发流程），也不是系统设计开发和实施所依据的产品开发流程。

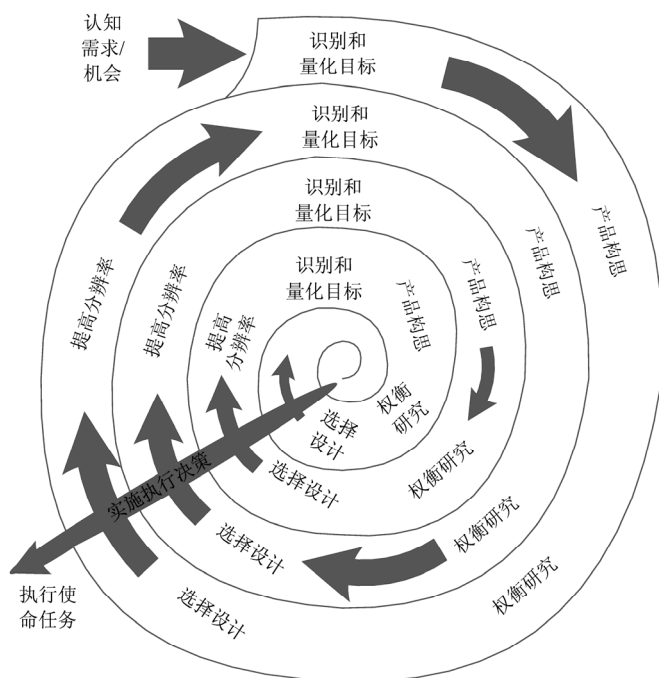


图 4.4-2 持续细化的理论

图 4.4-2 中每个产生构思的步骤都是由利益相关者期望驱动的递归和迭代的循环设计过程据此开发出系统架构/设计草案、相关的运行使用构想和派生的技术需求。这三个产品必须是相互一致的，如此需要反复的设计决策。这个迭代和递归设计循环如图 4.0-1 所示。

每个产生构思步骤也涉及到对技术状态持续改变产生的潜在能力进行评估，对根据以往工程/项目得到的经验经过基于经验的评审而获取的潜在缺陷进行评估。

在技术开发流程和设计流程之间持续交互以确保设计反映可用技术的真实性，并确保避免对不成熟技术的过度依赖是极其重要的。此外，对任何可能应用的技术必须进行适当的状态监控，且必须适时评估技术状态对产生构思过程的影响。这种交互通过在所需要技术的成熟度方面对设计进行的周期性评估得到促进（参见 4.4.2.1 节对技术评估更细致的讨论）。这些技术单元通常在产品分解结构的较低层次存在。尽管集成较低层次单元的设计构思开发流程是系统工程流程的一部分，但存在自顶向下的流程不能够同自底向上流程保持一致的危险。所以，系统架构问题需要在早期解决，这样系统能够通过充足的实际模型进行可靠的权衡研究。

随着系统设计的实施，系统特征也变得更加清晰，但也就更难改变。系统工程的目的是确保设计方案定义流程采用的方式能够引导完成效益最佳的系统。基本思想是在做出很难撤销的决策之前，对备选方案进行细致的评估，特别是考虑所需技术的成熟度。

2. 生成备选方案设计构思

一旦理解要完成的系统是什么，就要采取多种方式来实现这些目标。有时，接下来需要考虑备选方案功能分配和集成可用的子系统设计选项，所有这些都包含不同成熟度的技术。理想地考虑在不断细化的流程中，当前阶段位置需要定义可能的备选方案范围与设计组织工作性质的一致性。当实施自底向上的流程时，系统工程师面临的一个问题就是设计者都趋于欣赏他们创造的设计，从而丧失其客观性；系统工程师必须时常保持“局外人”角色以保证更加客观。这一点在评估子系统和组件的技术成熟度时特别重要。对部分技术开发者和项目管理层来说有个趋势，即过高估计实施设计所需技术的成熟度和可用性，对于既有设备尤其如此。结果就是系统工程的某些关键环节经常被忽视。

图 4.4-2 所示持续细化的第一轮中，主体通常是一般方法或策略，有时是架构概念。下一轮是功能设计，然后是设计细节等。避免不成熟地关注单独设计的原因是要发现真正的最佳设计。系统工程师的部分工作就是确保待比较的设计构思考虑所有的接口需求。“你考虑包含布线了吗”是一个典型的问题。在可能的情况下，每个设计构思应通过可控设计参数描述，这样每个参数可以尽可能合理地表述更多的设计类别。此刻，系统工程师应记住潜在的变更包括组织结构、进度表、技术规程，以及系统的其他任何组成部分。可能的话，约束条件也应该用参数描述。

1) 分析每个备选设计方案

技术团队分析每个备选设计方案满足系统目标的程度（技术缺陷、效能、成本、进度、风险、定量或非定量）。评估通过应用权衡研究来完成。实施权衡研究流程的目的是确保系统架构和设计决策在可用资源条件下达成最好的设计方案。这个流程的基本步骤如下：

- 设计备选的设计路线以满足功能需求。在项目寿命周期的早期阶段，该方法集中于系统架构；在后期阶段，集中于系统设计。
- 按照效能指标和系统成本对备选方案进行评价。这一步骤中数学模型很有用，不仅在辨明输出变量之间的关系方面，而且还在帮助决定哪些性能指标必须量化方面。
- 按照适当的选择标准对备选方案排序。
- 剔除不良方案，需要时推进到下一分辨率层次。

权衡研究流程必须开放地自始至终完成。即使是使用定量技术和规则，主观性同样起重要作用。为使流程工作有效，参与者必须头脑开放，有不同技能的个人（系统工程师、设计

工程师、专业工程师、工程分析者、决策科学家和项目负责人)必须相互合作。必须运用正确的定量方法和选择标准。权衡研究的假设、模型和结果必须作为项目档案的一部分存档。参与者必须时刻关注功能需求,包括支撑产品。关于权衡研究流程的深入讨论参见 6.8 节。实施研究的能力通过开发与评价设计参数相关(但不依赖)的系统模型得以提高。

开发系统模型时,技术团队必须考虑广泛的构思。模型必须定义系统中人员、硬件和软件的作用。必须确认完成使命任务的关键技术需求且必须考虑整个寿命周期,即从生产制造到退役处置。选择设计构思的评估标准必须建立。成本总是限制性因素,然而其他标准,如开发和认证元件的时间、风险和可靠性也很关键。不考虑操作者和维护者的作用,这个阶段就不能完成。这些对整个寿命周期费用和系统可靠性非常重要。可靠性分析要基于对硬件组件故障率的估计进行。如果运用风险概率评估模型,软件故障或人为操作失误的发生概率就很有必要包括进来。对所需技术成熟度的评估必须完成且要制定出技术开发计划。设计构思及系统模型的修正和开发应当可控,通常允许运用最优化技术来探索能促进进一步观察的设计空间。

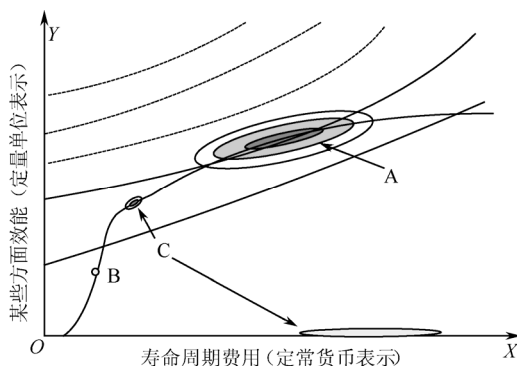
为进一步开发寻求最好的选择,不管系统模型使用与否,设计构思在一个闭合的循环过程中被开发、改进、再评估,并与竞争的备选方案比较。系统和子系统的尺寸通常在权衡研究中确定。最终结果是确定备选设计方案相关费效比的边界,使用量化的系统目标进行度量(因为刻意回避决定设计的最终细节,只可能获得边界,而非最终值)。随着不断改进的方案里相关细节的增加,流程推进时缩小了上界和下界之间的范围。

2) 选择最好的设计方案

技术团队从备选设计构思中选择最好的设计解决方案,其中考虑如下主观因素:团队在确定备选方案满足定量需求程度上,在评估可用技术的成熟度上,在确定任何效能、成本、进度、风险或其他约束条件上的量化能力并不比预估强更多。

决策分析流程,如 6.8 节所述,应该用于对备选设计构思进行评估,并且要推荐出最佳设计解决方案。

可能的话,开发称为“目标函数”的数学表达式是值得的,因为它把可能结果的综合值表述为一个单指标量:费效比,如图 4.4-3 所示,即使费用和效能需要多个指标量来描述。



注:不同阴影区域表示不同水平的不确定性。虚线代表目标函数(费效比)为常值。通过向左上方移动可以得到更高的费效比。A、B和C为不同风险类型下的设计构思。

图 4.4-3 定量目标函数,依赖于寿命周期费用和效能的所有方面

目标函数(或费用函数)在备选方案空间或“搜索空间”中为候选方案或“可行方案”赋一个实数值。这是使目标函数最小化(或最大化)的可行解决方案,即“最优方案”。当能

否达到目标可以用目标函数量化表达时，设计方案就可以按照它们的相应值进行比较。设计构思伴随的风险（因为不确定，最好用概率分布描述）可能使这些评价有些模糊。

在图 4.4-3 中，设计构思 A 的风险相对高些。构思 B 中效能或费用有很少的风险，而构思 C 有高代价失败的风险，如图中接近横轴的概率云团表示费用高且几乎没有效能。进度因素可能影响效能和成本值及风险分布。

系统使命任务成功标准有极大不同。在有些情况下，效能目标可能比其他的更重要。其他项目可能需要低成本、不可更改的进度表，或要求某类风险最小化。很少（如果有）可能产生组合的量化指标，其关联着所有重要因素，即使它表述为若干组分的矢量。就算能做到如此，重要的是彻底发现潜在因素和关系且被系统工程师所理解。系统工程师必须为那些无法量化的因素的重要性（像对量化数据那样）赋予权重。

数据和分析的技术评审，包括技术成熟度评估，是为技术团队准备决策支持材料的重要部分。所做的决策一般作为系统控制基线的变化或细节进入技术状态管理系统。权衡研究的支撑结果应被存档以备将来使用。系统工程流程的一个基本特征是权衡研究在做出决策之前执行。这样它们的控制基线能更准确地确定下来。

3) 提高设计方案的分辨率

图 4.4-2 所示的持续细化流程描绘了系统设计的不断细化。在分解的每个层次，将已确定控制基线的派生（和分配）需求变为一组被分解单元的高层需求，流程重新开始。可能有人问，“我们何时终止设计的细化？”答案是设计工作要推进到足够深度，以满足某些需要：设计要充分深入以允许对设计是否满足需求的定量确认；同样设计要有充分的深度以支持费用模型的应用，并在性能、成本和风险方面就设计可行性说服评审专家。

系统开发中系统工程引擎不断重复运用。随着系统的实现，考虑的问题和活动的特点都改变了。大多数大型系统决策（目标、架构、可接受的寿命周期费用等）在项目的早期阶段就完成了，接下来的细化并不精确地对应系统寿命周期的各个阶段。许多系统架构即使在开始时能够看清，但随后的细化也不能精确对应于所开发的架构层次。相反，它们对应系统被定义的后续更高分辨率的层次。

期望系统随时间有更高分辨率的定义是合理的。这个趋势在（阶段 B）某个点上通过控制基线的系统定义而形式化。通常，设定控制基线时，目的、目标和约束条件作为控制基线的需求部分。完整的控制基线遵从技术状态控制以试图确保任何后续变更确实是正当且可接受的。在系统工程流程的这个点上，有个逻辑分支点。对于推进了足够远的后续细化流程所碰到的问题，下一步是在当时分辨率层次进行决策。对于那些仍不能充分解决的问题，需要进一步细化开发。

4) 完整描述设计方案

一旦合意的设计备选方案被选定且完成了适当层次的细化，则设计被完整地定义成满足技术需求的最终设计解决方案。设计方案定义将用于生成目标产品规范，该规范用于生产产品和进行产品验证。这个流程依赖于待定义目标产品是否有附加的子系统来进行进一步细化。

完整设计描述的范围和内容必须适用于产品的寿命周期、阶段成功准则及产品在产品分解结构中的位置。依赖于这些因素，设计方案定义的形式可以简化为一个仿真模型或研究报告。技术数据包按照阶段演化，从概念草图或模型开始，到形成完整的图样、部件清单及产品生产或集成所需要的其他细节时结束。设计方案定义流程的典型输出定义如图 4.4-1 所示，且在 4.4.1.3 节中描述。

5) 验证设计方案

一旦从多种备选设计中选定可接受的设计方案且在技术数据包中记录, 接下来设计方案就必须根据系统需求和约束条件完成验证。进行验证的方法是通过同行评审来评价选定的设计方案。进行同行评审的指南在 6.7 节讨论。

同行评审作为高层次技术和程序评审的一个详细技术部分起重要作用。例如, 对电池组件设计的同行评审与能源子系统的集中评审相比, 能探究关于电池的更多技术细节。同行评审覆盖从子系统到系统组件相应层次, 根据需求进行设计验证。同行评审所关心的问题, 可能涉及能源子系统的设计和验证方面, 所以必须向能源子系统的后续更高层次提交评审报告。

验证必须表明设计方案定义能做到如下所述:

- 在技术工作的约束条件内能够实现。
- 有详细的以可接受的方式表达的需求陈述, 在派生的技术需求、分配的技术需求和利益相关者期望之间有双向可追溯性。
- 形成解决方案时的决定和假设与派生的技术需求、分配的技术需求, 以及确认的系统产品和服务约束相一致。

设计解决方案的验证和目标产品的验证形成对照, 后者在技术数据包中的目标产品验证计划中描述。验证发生在寿命周期的后期阶段, 是产品验证流程的结果 (参见 5.3 节), 运用在作为目标产品的设计方案实现中。

6) 设计方案确认

设计方案确认是个迭代和递归的过程。每个备选设计构思根据利益相关者期望来确认。利益相关者期望驱动设计的循环迭代, 以开发结构/设计草案、运行使用构想和派生的需求。这三个产品之间必须相互一致, 且需要反复设计决策来达到这种一致。一旦达到一致, 研发团队可以采用功能分析方法根据利益相关者期望来确认设计。简单化的确认询问如下问题: 系统能否运行? 系统是否安全和可靠? 系统费用能否承受? 如果任何一个问题的答案是否定的, 就需要变更设计或利益相关者期望, 流程就要重新开始。这个流程持续进行直到系统的结构、运行使用构想和需求都满足利益相关者的期望。

设计方案的确认与目标产品的确认形成对照, 后者在技术数据包中的目标产品确认计划中描述。确认发生在寿命周期的后期阶段, 是产品确认流程的结果 (参见 5.4 节), 运用在目标产品的设计方案实现中。

7) 确定辅助产品

辅助产品是为全寿命 (如生产、测试、部署、训练、维护和处置) 提供支持, 并能够促进目标产品全寿命周期运行使用的产品和服务。目标产品及其辅助产品是相互依赖的, 可以看做一个系统。这样, 项目的职责延展到在寿命周期每个阶段从相关的辅助产品获取服务。当合适的辅助产品尚不存在时, 对目标产品负责的项目, 同样要对制造和使用辅助产品负责。

所以, 在设计方案定义流程中一个重要的活动就是根据寿命周期中选定的设计方案确定辅助产品, 促成这些辅助产品的采购或开发。需要应用辅助产品的日期必须实际地标注在项目进度表中, 并允许适当的进度延迟。同时以合同、协议、使用计划等形式规定的义务必须确定下来, 以确保辅助产品在需要支持产品寿命周期活动时是有效的。辅助产品需求应当作为设计方案定义流程中技术数据包的一部分归档。

环境测试箱可作为一个辅助产品的例子, 它在空间飞行系统试验阶段的适当时候需要使用。

专门的测试装置或专门的机械操作装置也可作为辅助产品的例子, 它们必须由项目制

造。由于开发时间很长及订购的设施过多，确定辅助产品并确保尽可能在设计阶段早期确定其义务是很重要的。

8) 设计方案控制基线

一旦选定的系统设计方案满足利益相关者期望，研究团队即确定产品控制基线，并准备进入产品寿命周期下一阶段。由于设计细化工作的递归特性，分解的中间各层通常作为流程一部分来验证和确定控制基线。在向下层的分解中，待分解高层单元的需求变为确定控制基线的需求，并且流程重新开始。

确定特定设计方案的控制基线使技术团队在所有备选设计构思中专注于单个方案。这是设计流程的关键点。它相当于建立了一个基础，使设计团队每个人都关注同一构思。当处理复杂系统时，如果系统设计目标改变，会造成团队成员在完成所负责的系统设计部分的困难。控制基线已确定的设计方案被归档并置于技术状态控制下。这包括系统需求、规范和技术状态描述。

即使确定设计控制基线对设计流程有益，但若它在设计方案定义流程中运用过早则存在危险。备选设计方案的早期探索应该是自由和开放的，具有广泛的思路、概念和方法。控制基线确定过早，概念探索就会缺少创造性。因此，确定控制基线应该是设计方案定义流程的最后一步。

4.4.1.3 输出

设计方案所定义流程的输出是提交到产品实施执行流程的规范和计划，包括产品设计、建造和编码的相关文件、遵从系统被批准的控制基线。

如前文所述，完整设计描述的范围和内容必须适合相关产品寿命周期阶段，服从阶段成功准则和产品在产品分解结构中的位置。

设计方案定义流程的输出如下所述。

- **系统规范：**系统规范包括作为设计方案定义流程结果的系统功能控制基线。其中，系统设计规范为设计工程师开展系统设计工作提供充分的指南、约束条件和系统需求。
- **系统外部接口规范：**系统外部接口规范描述系统与外部世界之间的所有物理接口行为和特征的功能控制基线。这些接口包括所有结构接口、热交换接口、电路接口、信号接口及人机系统接口。
- **目标产品规范：**目标产品规范包括详细的目标产品如何建造和如何编码的需求。它们是对设计细节详细而准确的表述，如规定原料和尺寸，以及建造或组装目标产品工作的质量等表述。
- **目标产品接口规范：**目标产品接口规范包括目标产品与外部单元之间的所有逻辑接口和物理接口（包括人机接口）在其相关行为和特性方面如何构建和如何编码方面的需求。
- **初始子系统规范：**目标产品子系统的初始规范在需要时提供关于子系统的详细信息。
- **辅助产品需求：**辅助产品需求支持提供所有辅助产品的细节。辅助产品是为产品寿命周期提供支持的产品和服务，可促进相应目标产品在其寿命周期的进展和运用。它们被认为是系统的一部分，因为目标产品及其辅助产品是相互依赖的。
- **产品验证计划：**目标产品验证计划确定为保证目标产品全部验证活动完整可视性所需的内容和详细程度。根据目标产品的范围，该计划包含对飞行器硬件和软件的鉴定、验收、射前、使用和处置等相关的验证活动。

- **产品确认计划：**目标产品确认计划确定为保证已实现产品与利益相关者期望控制基线之间全部确认活动的完整可视性所需的内容和详细程度。该计划包括确认的类型、确认的技术规程，以及适合于证实已实现目标产品符合利益相关者期望的确认环境。
- **后勤保障和使用技术规程：**可行的系统后勤保障和操作使用技术规程描述相应设计方案在控制、运输、维护、长期储存和使用方面需考虑的事项。

4.4.2 设计方案定义指南

4.4.2.1 技术评估

如在流程描述（参见 4.4.1 节）中所提及的，生成备选设计方案涉及对不断变化的技术状态所提供潜在能力的评估。在技术开发流程和设计流程之间的不断交互可确保设计反映现实可用的技术。通过在完成设计所需要的技术成熟度方面对设计进行定期评估，这种交互得以加强。

对于特定的设计构思，在明确其中技术缺口之后，经常有必要采取技术开发措施以确保设计的可行性。通常情况下资源总是有限的，所以，有必要追求最有希望的技术以满足特定设计构思的需要。

如果没有完整地理解完成技术开发所需要的资源而进行需求定义，那么工程/项目就处于风险中。技术评估必须反复进行直到需求和可用资源都处在可接受的风险范围之内。技术开发在工程/项目寿命周期内所起到的作用远比传统上想象的更大，帮助加深对工程/项目更广阔影响（效益最大化和负面作用最小化）的理解是系统工程师的职责。传统上，从工程/项目的角度看，技术开发总与为满足需求所需的“新”技术开发和技术引进相关。然而，对原有系统的修改可能导致不同的系统架构和与设计不同的系统使用环境这种情况却经常被忽视。如果需要的系统修正和/或使用环境超出已有的经验，此时应该慎重考虑是否进行技术开发。

为了了解是否需要进行技术开发，进而量化相应的费用、进度表和风险，有必要按照架构和使用环境对每个系统、子系统或组件的成熟度进行系统地评估。这样就有必要评估需要开发什么才能够将成熟度提升到相应水平，能够顺利地与费用、进度表及性能等约束条件相适应。完成这个评估的流程在附录 G 中描述。因为技术开发对工程/项目有潜在的显著影响，技术评估必须从概念开发到初步设计评审的设计和开发流程中起到作用。从技术开发观点看，这有助于在工程的最后阶段总结经验教训。

4.4.2.2 在系统工程流程中需集成的工程特性

作为技术工作的一部分，专业工程师通常与系统工程师和子系统设计师合作，执行跨学科的工作任务。首先，他们运用专门的分析技术提供项目负责人和系统工程师所需要的信息。他们同样帮助在其专业领域内定义和撰写系统需求；他们评审数据包、工程变更需求、测试结果和主要的项目评审文档。项目负责人或系统工程师需要确保生成的信息和产品对项目的附加价值与其成本相当。专业工程技术工作应很好地集成在项目中。专业工程技术学科的作用和职责也应在系统工程管理计划中概述。

本手册中包含的专业工程技术学科有安全性、可靠性、质量保证、综合后勤保障、维修性、可生产性和人因工程。这里给系统工程师提供这些专业工程技术学科的总体简明介绍，不刻意成为这些学科专业的手册。

1. 安全性和可靠性

1) 概述和目的

可靠的系统通过适当确定其预期寿命以确保使命任务成功。可靠系统的失败概率很小且可以接受，通过简化、适当设计、可靠元件及原料的适当运用来实现。除长寿命外，可靠系统是健壮的和容错的，即它能容许操作参数及运行使用环境的错误和变化。

2) 系统设计过程中的安全性和可靠性

关注使命任务的安全性和可靠性对确保使命任务成功是必要的。系统安全性和可靠性的设计和实现的逼真度依赖于所需信息和使命任务类型。对载人系统，安全性和可靠性是贯穿设计过程的主要目标。对于科学使命，安全性和可靠性要与工程或项目的资金和能承受的风险相对称。不论使命任务的类型如何，安全性和可靠性考虑都必须是复杂的系统设计流程中一部分。

为实现可靠性分析的利益最大化，在设计团队中加入风险和可靠性专家是必要的，这一点毫不夸张。多数情况下，可靠性和风险分析师在设计方案形成后对其进行分析。此时，安全性和可靠性特征是额外加入的而非设计出的。这可能导致不切实际的分析，设计中没有关注风险源，而分析也没有为设计提供价值贡献。

风险和可靠性分析需要回答设计权衡和成熟度的关键问题。可靠性分析利用系统信息识别风险和风险源，并且为决策提供重要的输入。NASA-STD-8729.1《规划、开发和维护有效的可靠性和维修性（R&M）工程》概述了每个特定项目可以剪裁的工程技术活动。其概念是选择可靠性和维修性工程技术活动的有效集以保证系统设计、建造和部署能针对所需的使命任务周期成功进行。

在项目早期阶段，风险和可靠性分析帮助设计者理解需求、约束条件和资源的相互关系，揭开关键关系和动因，便于适当地分析。分析人员必须帮助设计人员在需求之外理解设计构思成熟时显现的内在依赖关系。假设设计需求能够准确获取所有风险和可靠性问题，并且能够得到可靠的设计方案是不现实的。系统工程师应当开发与产品分解结构相对应的系统战略，说明如何在系统纵向和水平结构上分配和协调可靠性、容错性及恢复能力以满足整个使命任务的需求。设计方案的系统影响在设计中起着关键作用。使设计者感知其决策对整个使命任务可靠性的影响是关键。

随着设计的成熟，运用确定的技术进行初步可靠性分析。设计方案和运行使用构想应做彻底地检查，因为事故苗头或隐患将会导致灾难。对危险发生可能性和结果的保守估计可作为运用设计资源来缩减失败风险的基础。设计团队也应在整个系统中确保目标能够满足并考虑相应的失效模式。

在项目的后期阶段，设计团队运用风险评估和可靠性技术检验设计方案是否满足其风险和可靠性目标，帮助开发当目标不能满足或偏差/失效发生时的风险缓解策略。

3) 分析技术和方法

可靠性分析技术和方法的简单概要的分类如下：

- 事件序列图/事件树都是描述事件序列和使命任务中可能发生未知情况响应的模型。
- 失效模式和影响分析（FMEA）是自底向上的分析、辨识系统可能发生的失效类型，并且辨识失效原因、影响和用于控制失效影响的缓解策略。
- 定性的自顶向下的逻辑模型辨识系统失效组合如何能引起意外事件的发生。

- 定量的逻辑模型（概率风险评估）扩展定性模型，包含了失效的可能性。这些模型涉及基于系统物理性质和系统成功准则开发失效准则，且应用统计技术评估不确定条件下失效的可能性。
- 可靠性框图是评估系统提供某项功能可靠性的元素构成的逻辑框图。
- 预先危险分析（PHA）基于使命任务中功能表现尽早进行。预先危险分析是个确定“万一怎么办”的过程，考虑潜在的危险、初始事件想定和影响，以及可能的调整和控制措施。目标是决定危险是否能排除，不能排除时如何进行控制。
- 危险分析用于评价已完成的设计。危险分析是个确定“万一怎么办”过程，考虑潜在的危险、初始事件影响和可能的调整和控制措施。目标是决定危险是否能排除，不能排除时如何进行控制。
- 人员可靠性分析是了解人为失误如何导致系统失效且评估这些失效可能性的方法。
- 概率结构分析提供结合材料和载荷的不确定性来评估结构单元失效的方法。
- 备件/后勤保障模型提供实时评估系统交互的方法。这些模型包括地面过程仿真和使命任务活动仿真。

4) 可靠性分析的局限性

工程设计团队必须理解可靠性可表述为使命任务成功的概率。概率是对特定事件发生可能性的数学度量。因此，概率估计应当基于工程技术和历史数据，并且在估算过程中任何既得概率应包括某种不确定性的估量。

不确定性表述分析者对其所做估计的置信程度。随着数据质量和对系统理解的提高，不确定性相应减少。失效率或失效概率的初始估计可能基于相似设备、历史（继承）数据、手册中失效率数据或专家诱导。

总之，可靠性估计用于表达成功的概率。不确定性应包含在可靠性估计中。可靠性估计与 FMEA 结合为辅助决策流程提供附加的且有价值的信息。

2. 质量保证

即使是最好的设计，硬件制造和测试都可能遭遇人为错误。系统工程师需要相信系统实际上是依照它的功能需求、性能需求和设计需求生产和提交的。质量保证在项目寿命周期中为项目负责人和系统工程师提供产品生产和流程使用的独立评估。项目负责人和系统工程师必须与质量保证工程师一起工作，开发适合相应项目的质量保证计划（质量保证活动的范围、责任和时间）。

质量保证是 NASA 工程实践的质量支柱。NPD 8730.5《NASA 质量保证计划政策》中阐述的 NASA 政策为“在质量保证计划实施中，工作性能符合既定需求，并且提供独立灵活的担保”。安全性与使命任务担保书中的质量功能用于保证承包商和其他 NASA 单位按照其承诺和进行的工作准备开展工作。这确保了目标产品和工程的质量、可靠性和全部风险在计划规定的水平上。

系统工程师与质量保证的关系

同可靠性、可生产性和其他特征一样，质量必须作为系统的集成部分设计。对于系统工程师来说，理解使命任务担保书在全面风险环境下的安全防护作用，并明确支持质量的作用。如果有效地考虑了使命任务担保书的质量功能，如果从概念开发阶段开始，所有的设计都符合质量要求，这就比较容易。这有助于缓解设计需求和质量需求的冲突，体现出“容差累积”的效果。

质量是风险管理的关键部分。错误、偏差、遗漏和其他问题可能要消耗时间、工程资源、纳税人的钱甚至生命。了解质量如何影响项目并鼓励以最优方法达到质量水平的要求，是系统工程师的职责所在。

严格坚持规划的需求对高风险、低容量的制造是必要的。缺少大的样本和长时间的生产，依照这些书面技术规程对确保流程及产品的一致性是非常重要的步骤。为说明这点，NASA 要求设计质量保证计划来缓解不符合这些需求的风险。这样可能生成大量需求和技术规程。这些必须分解到供应链，甚至到最底层的供应商。对于不符合需求而导致生命损失和使命任务失败的情况，应在政府强制检查技术规程中嵌入相应需求，以确保 100% 的满足安全性/使命任务的关键属性。安全性/使命任务关键属性包括硬件特性、制造流程需求、运行使用条件、功能实现标准，如果不满足将可能导致生命损失和使命任务失败。

按照联邦采办法规（FAR）第 46.4 节的要求制定适当的工程/项目质量保证监督计划。NPR 8735.2《NASA 合同的政府质量保证功能管理》中概述了工程/项目质量保证监督计划的准备和内容。该文件涵盖低风险和高风险采办的质量保证需求，并且包括文档评审、产品检查、流程见证、质量系统评价、违规报告和纠正行动、质量保证和监督的计划，以及政府强制检查点等功能。此外，多数 NASA 项目坚持 ISO9001（非关键工作）或 AS9100（关键工作）的质量系统管理需求标准。对于大多数 NASA 职能，质量系统培训是强制的，因此，假设系统工程师应当具备这些系统的能力知识。它们的文本和意图完全反映在 NASA 的质量技术规程文档中。

3. 综合后勤保障

系统工程流程中综合后勤保障活动的目标是确保产品/系统在（阶段 D）开发和（阶段 E）使用中以有效的方式得到保障。综合后勤保障的重用性和持久性对项目特别重要。对于主要产品尚未进展到使用阶段的项目，其综合后勤保障仅应用于项目的部件（如地面系统）或某些单元（如运输系统）。综合后勤保障基本上通过早期实时考虑保障性特性，对备选系统和综合后勤保障进行权衡研究，量化使用最佳方案的每个综合后勤保障单元的资源需求，获得与每个综合后勤保障单元相关的保障产品来完成。在使用阶段，综合后勤保障活动支持系统通过分析实际运行使用条件，并不断修改综合后勤保障系统及其资源需求，寻求效费比的提高。忽视综合后勤保障或低劣的综合后勤保障决策总是对相关系统寿命周期成本有负面影响。表 4.4-1 对综合后勤保障的技术内容进行了概要总结。

表 4.4-1 综合后勤保障的技术内容

技术内容	定义
维护保障计划	必要的计划、组织和管理活动的进行和反馈，确保既定工程的后勤需求能适当地调整和实现
设计接口	后勤保障和系统工程流程的交互和关系，确保保障性对系统定义和设计的影响能够降低寿命周期费用
技术数据和技术发布	记录科学的、工程的、技术的和成本的信息以用于系统的定义、生产、测试、评价、修正、部署、保障和运行
训练和训练保障	包括所有必要的人员、设备、设施、数据和记录及辅助资源，用于使用人员和维护人员的训练
供应保障	提供所有必须的材料以确保系统保障性和可用性目标实现所需要的行动
试验和保障设备	所有需要的工具、条件监控设备、诊断和检验设备、特殊试验设备、度量和校准设备、维修器械和维修台及控制设备，用于维护运行使用的功能

续表

技 术 内 容	定 义
包装、处理、存储和运输	所有需要的材料、设备、特殊设备、容器（可重用和可处置）和物品，用于支持与使命任务相关主要单元的包装、安全性和保存性、存储、加工和运输，包括人员、备件和维修件、试验和保障设备、技术数据计算机资源和可移动设施
人员	涉及识别和获得具备在系统寿命周期中使用和维护系统的技能和等级的人员
后勤保障设施	支持后勤保障活动需要的所有专用设施，包括存储建筑和仓库，以及各种维护设施
计算机资源保障	所有必要的计算机、相关软件、连接组件、网络及接口，用于保障所有后勤保障功能日常需要的信息流

综合后勤保障计划应该在项目寿命周期早期开始和记录。这个计划应说明表 4.4-1 中包含的要素是如何考虑、执行和集成到系统工程流程需求中的。

4. 可维修性

可维修性被定义为一个产品组件在特定条件下，即由具有特殊技能水平的人员，使用预定的技术规程和资源，在预定的维修层级进行维修时，保持和恢复其能力的度量。采取维修行动时的方便性、经济性、安全性和精确性是设计或安装的固有特性。

维修性工程师的作用

维修性工程是另一个主要的专业学科，其目标是可保障系统。维修性工程在系统工程流程中完成，在预定物理环境下产品特定设计特征的实施活动中起主要作用，促进安全和有效的维护行动，并在综合后勤保障系统开发中起核心作用。维修性工程师的任务包括如下示例：开发和维护系统维修概念，建立和分配维修性需求，进行分析以量化系统的维护资源需求及验证系统的可维修性需求。

5. 可生产性

可生产性是与便捷和经济相关的系统特征，基于此，所完成的设计能够（通过构造、制造或编码）转化为硬件产品或软件产品的实现。由于多数 NASA 系统一般仅需要少量生产，特殊的可生产性特征对系统的费效比很关键，如航天飞机隔热瓦的生产和使用经历所表明的。影响设计可生产性的因素包括原料的选择、设计的简化、产品方案的灵活性、严格的容差需求和技术数据包的简化。

生产性工程师的作用

生产性工程师（作为多学科产品开发团队的成员）辅助系统工程流程，在实施专门设计特征来增强可生产性及在进行项目需要的产品工程技术分析中起积极作用。这些任务和分析如下：

- 执行系统风险管理计划关于制造/建造的部分。通过进行严格的产品风险评估和计划有效的风险缓解活动来完成。
- 确认系统提高可生产性的设计特征。工作重心在于设计简化、建造容差和避免危险材料。
- 进行可生产性权衡研究，决定具有最佳效益的建造/制造流程。
- 在项目约束条件内评估生产可行性。这可能包括评估承包商和主要分包商生产经验和能力、新的建造技术、特殊工具和生产人员的训练需求。

- 确认长效构件和关键原料。
- 估计生产成本，作为寿命周期费用管理的一部分。
- 支持成熟度评估。
- 开发生产进度表。
- 开发建造/制造流程确认的方法和计划。

这些任务和生产工程技术分析的结果记录在生产计划中，项目各阶段详细度适中。生产性工程师还参与针对上述事项的项目评审（主要是初步设计评审和关键设计评审），以及特殊的临时评审如生产技术成熟度评审，并提出自己的观点。

6. 人因工程

1) 概述和目的

考虑系统的人为操作和维护是设计流程的关键部分。人因工程是研究人与系统接口，并提供需求、标准和指南，确保集成在系统中的人类组件能够像预期那样发挥功能的学科。人的角色包括操作者（飞行乘员和地面人员）、设计人员、制造人员、地勤人员、维护人员和乘客。飞行乘员的职能包括系统操作、发现故障、飞行中维护。地面人员的职能包括空间飞行器和地面系统制造、组装、测试、校验、后勤保障、地面维护、修理、翻新、发射控制和使命任务控制。

人类因素大体上分为四种。第一种是人体测量学和生物力学——物理尺寸、形状和人的力量。第二种是感觉和感知——主要是视觉和听觉，触觉等感觉也很重要。环境是第三种因素，包括周边噪声和光线、振动、温度与湿度、大气成分和污染。第四种是心理因素，由记忆、信息处理组件如模式识别、决策、信号探测，以及情感因素——如情绪、文化和习惯等组成。

2) 系统设计流程中的人因工程

- **利益相关者期望：**操作人员、维护人员，以及乘客都是系统的利益相关者。人因专家确认能够由人类和超出人类能力的想定所承担的角色和责任。人因专家确保系统运行使用构想的开发中包括任务分析和人/系统的功能分配。随着不断细化，功能分配将操作人员的角色和责任分解为乘员、外部保障团队，以及自动化设备相应的子任务（例如，飞行中任务可能分解到乘员、空中交通管理或自动驾驶仪。对于空间飞行器，任务可能由乘员、使命控制或其他星载系统执行）。
- **需求定义：**根据 NASA-STD-3001《NASA 空间载人飞行系统标准第 1 卷：宇航员健康》，对宇宙飞船和太空舱的人因需求是与项目相关的。其他使命任务和人类空间飞行的地面活动中，人因需求由 MIL-STD-1472《人因工程》和 NUREG-0700《人与系统接口设计评审指南》，以及《联邦航空管理局人因设计标准》等人因标准获得。
- **技术方案：**在逻辑分解和开发设计构思时将人因考虑为中心组件。作为用户的操作人员或维护人员无法像设计人员那样能看到完整系统，而只能看到系统与其接口的部分。在工程设计评审中，人因专家促进设计方案的可用性。尽早考虑能使人因评估捕获工程早期的使用性问题。例如，在某国际空间站有效载荷设计项目中，装载量和硬件早期布局模块图的人因评估识别了可能使操作非常困难的问题。在费用可忽略的情况下对概念设计做出变更——即基于用户访问序列重新安排概念框图，保证用户的可操作性。

- **设计构思的可用性评价：**使用硬件和软件接口快速原型工具、标准的人因工程数据收集和分析工具，以及相应指标如任务完成时间和错误数量等，评估很容易完成。从操作人员那里系统地收集主观报告同样能提供有用数据。需采用能提供详细客观信息的技术，如通过肉眼观察对显示和控制面板布局进行评估。人因专家的作用是在反复的设计过程中提供评估能力。
- **验证：**如上所述，对可用性、故障率、任务完成时间和工作量的需求验证是富有挑战性的。验证方法覆盖从在样机和模拟器上测试训练人员，到建立人的性能模型，再到专家调查。作为系统工程团队成员，人因专家最早应从需求开发时提供验证指导。

3) 人因工程的分析技术与方法

用于提供人工效率数据，预测人与系统的性能，评价人与系统设计的方法示例如下所述。

- **任务分析：**对人在系统中为完成任务必须做的事项进行详细描述，强调对信息表现、决策、任务时间、操作动作和环境条件的需求。
- **时间线分析：**来自于任务分析。在任务分析中任务持续时间被确认，并且用图示表示这些任务的发生时刻，同时显示任务顺序。目的是辨识不能同时发生的活动和耗时超过许可的活动需求。给定任务的时间线可以描述多个操作人员和乘员的活动。
- **建模和仿真：**为预测系统性能、比较系统技术状态、评价技术规程和评价备选方案建立模型或样机。仿真可以采用简化的模型，如确定人体外在特征和位置的图形化人类模型，也可以是复杂的随机模型以获取决策点和误差可能性等。
- **可用性试验：**基于任务分析和初步设计，在带有监视和记录设备的可控环境下执行实际任务。对客观指标（如完成时间和错误数量）进行评价，同时积累主观评估。测试结果系统地报告关于备选设计方案的优缺点。
- **工作量评估：**工作总量和工作类型的标准化尺度度量，如采用 NASA 工作量评估工具 NASA-TLX 或库珀-哈伯等级度量^①。它评估操作人员和乘员的任务量，确定相关人员在给定时间内以给定精度执行给定任务的能力。
- **人为错误和人类可靠性评估：**自顶向下（故障树）和自底向上（人因流程失效模式和影响）的分析。目标是创造能容忍和恢复人为错误的系统来提升人员可靠性。该系统必须支持将人的作用加入到系统可靠性中。

4) 人因专家的作用

在设计、生产和使用阶段，人因专家通过描述用户和维护人员的需求和能力来支持系统工程流程。人因专家的作用如下：

- 在需求定义阶段基于 NASA 标准确认关于人与系统集成的可用需求。
- 通过提供人员执行能力和局限性信息，支持使命任务概念开发。
- 基于人员能力和局限性信息支持任务分析和功能分配。
- 确认增强可用性的系统设计特征，这需要集成人员执行能力和设计特征的知识。
- 通过在备选方案对完成任务时间、工作量和错误率的影响方面提供数据，支持权衡研究。
- 通过在备选方案对操作系统所需技巧和训练的影响方面提供数据，支持权衡研究。

^① *库珀-哈伯等级（Cooper-Harper Rating Scales）是飞行测试工程师和试飞员用于测试评价新型号飞机操控性能的评价等级标准，共分为 10 各等级，等级 1 表示最佳的操控性能，而等级 10 表示最差的操控性能。

- 辅助进行设计评审，确保其服从人与系统的集成需求。
- 使用样机和原型进行评价，提供用户性能的详细数据。
- 与硬件设计人员和使命任务计划制定人员协同，支持训练和维护技术规程的开发。
- 收集使用中人与系统集成问题的数据，为未来设计做准备。

原 型

经验表明，即使在建造单一的飞行系统时，原型系统也可以有效地增强生产效率。原型在寿命周期早期建造，并尽可能在相应开发阶段与飞行构件在形式、外表和功能上一致可行。原型用于“描绘出”设计方案，从原型得到的经验能够反馈到设计变更中，从而提升单一飞行构件的制造、集成和维护水平，或若干飞行构件的生产运行能力。然而，原型经常因为需节省费用而从项目中删除。这样的决策增加了项目寿命周期开发阶段的风险。幸运的是，计算机辅助设计和制造技术的进步在某种程度上降低了这些风险，使得设计者将设计可视化为“按部就班”的集成步骤，在引起高费用的问题成为现实之前发现它们。

第5章 产品实现

本章描述图 2.1-1 中列出的产品实现流程中的各项活动。本章根据图 2.1-1 中的步骤 5~9 步骤相应划分小节。图中每一步流程按照输入、活动和输出进行讨论。与 NASA 项目相关的附加指南结合实例给出。

系统工程引擎右半部分给出产品最终实现流程。在引擎的该部分中，5 个相互依赖的流程使得系统能够满足设计规范与利益相关者期望。产品通过生产、购买、重用或编码，在较高层次组装集成，根据设计规范验证，根据利益相关者期望确认，最终提交到系统的更高层次。如前所述，产品可以是模型与仿真、纸质研究报告或建议，或是硬件与软件。产品的类型和层次取决于寿命周期阶段和产品特定目标。不论什么产品，必须有效地使用这些流程，以确保满足既定的运行使用构想。

产品实现工作始于技术团队获得系统设计流程的输出，并应用交叉关联的技术（如数据及技术状态管理）和技术评估方法，生产、购买、重用子系统。子系统一旦实现，必须集成到相应接口需求指定的适当层次中。随后这些产品经过技术评估流程验证，确保其与技术数据资料的一致性，即确保产品被正确地建造。若达到一致性要求，技术团队根据利益相关者期望对产品进行确认，确保建造的是正确的产品。在成功完成确认的基础上，产品提交到系统的更高层次。图 5.0-1 给出了这些流程。

这是一个迭代递归流程。纸质产品、模型和仿真贯穿 5 个实现流程之中。随着系统在寿命周期中的成熟与发展，硬件和软件产品亦贯穿这些流程。重要的是应在产品集成的最低层次上和寿命周期早期发现失误与不足，如此可以在设计流程中做出对项目影响最小的变更。

后续各节分别描述 5 个实现流程及其针对给定 NASA 使命任务的相关产品。

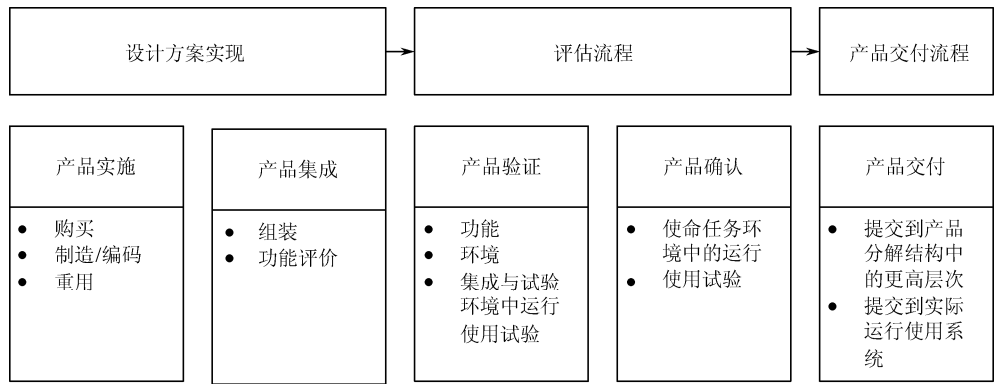


图 5.0-1 产品实现

5.1 产品实施执行

产品实施执行是系统工程中产品实现相关流程的第一个，从产品层次结构的最底层向

上，直到产品交付流程。这是将产品的计划、设计、分析、需求开发及设计图纸实现为实际产品的流程。

产品实施执行通过购买、制造/编码、重用前期开发的硬件、软件、模型或研究成果，生成项目和活动的特定产品，从而生成寿命周期阶段的相应产品。产品必须满足设计方案及其特定需求。

产品实施执行流程是项目从计划与设计推进到产品实现的关键活动。根据项目需求和项目寿命周期阶段，产品可能是硬件、软件、模型、仿真、样机、研究报告或其他实际结果。这些产品可以通过在商户和货商处购买实现，或自主研制开发，或通过部分/完整重用其他项目或活动的产品实现。对项目所需产品实现方式的决策，或这些实现方式组合的决策，应当在寿命周期早期通过应用决策分析流程做出。

产品实现的关键

- 生成并管理与其他产品相关的硬件与软件现货产品的需求。
- 了解验证试验与确认试验的区别。
 - **验证试验：**验证试验与批准的需求集（如系统需求文档）相关，可以在产品寿命周期的各个阶段开展。验证试验包括（1）用于辅助产品、产品单元的开发及不断成熟，或辅助产品生产和保障流程的任何试验；（2）任何用于验证技术成熟状态、验证设计风险最小化、证实达到合同中要求的技术性能、认证试验准备就绪的工程技术型试验。验证试验使用仪器和测量设备，通常由工程师、技术人员、运行维护试验人员在受控环境中完成，以便进行缺陷分析。
 - **确认试验：**确认与运行使用构想文档相关。确认试验在真实环境或模拟环境下针对所有目标产品进行，目的是确定典型用户在使命任务中运行使用的产品的有效性和适用性，并对试验结果进行评价。试验是详细量化的验证和确认方法。任何情况下，对将生产与部署的目标产品必须进行确认试验。
- 在评价为达成成功产品交付所需输入时，应考虑所有客户和利益相关者，以及技术的、工程的和安全性需求。
- 尽可能早地分析所有潜在的接口不兼容性。
- 完整了解并分析所有试验数据，发现趋势与异常。
- 理解试验和所做假设的局限性。
- 确保重用产品在当前系统应用时满足所需的验证和确认，而不只是依赖于其在原应用系统中满足的验证和确认。对于购买的产品和自制的产品，应当满足相同的验证和确认要求。重用产品的“出身”在不同的系统、子系统和应用中是不可依赖的。

5.1.1 流程描述

图 5.1-1 给出了产品实施执行流程的典型流程图，以及产品实施执行所需考虑的典型输入、输出和活动。

5.1.1.1 输入

产品实施执行活动的输入主要依赖于有关目标产品是否通过购买获得，或自主开发，或通过部分/全部重用其他项目产品形成的决策。典型输入如图 5.1-1 所示。

- **购买目标产品时的输入：**如果做出购买部分或全部项目产品的决策，目标产品的设计规范可从技术状态管理系统，以及其他相关文档（如系统工程管理计划）中获得。

- **制造/编码目标产品时的输入：**对于由技术团队制造/编码的目标产品，输入可能是技术状态控制下的设计规范和由项目提供或购买的原材料。
- **重用目标产品所需的输入：**对于部分或全部重用其他项目现成产品的目标产品，输入可能是产品相关文档及产品本身。必须注意确保重用的产品确实满足项目的设计规范和运行环境。这可能是决策分析流程中做出购买/自研/重用决策的影响因素。

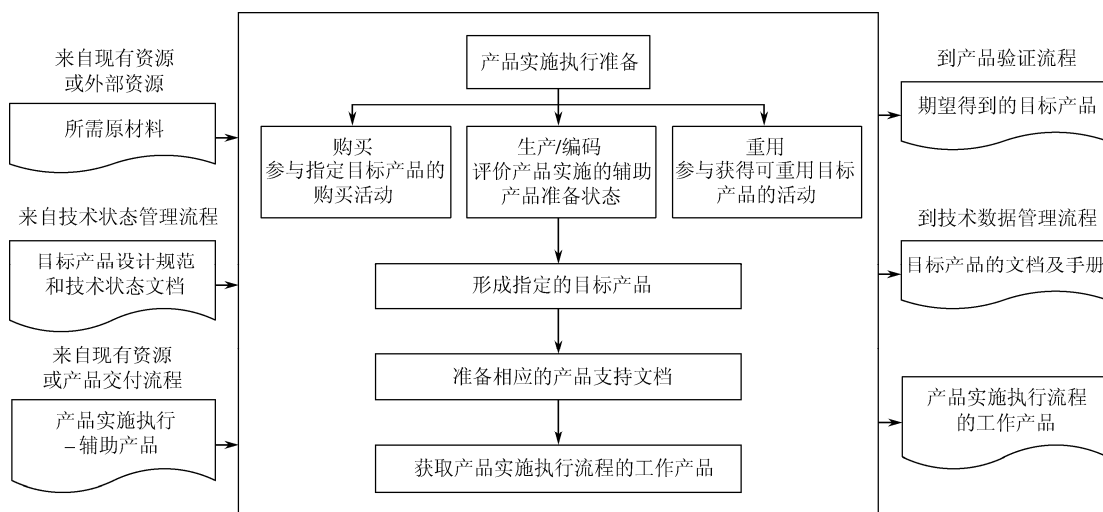


图 5.1-1 产品实施执行流程

5.1.1.2 流程活动

产品的实施执行的三种方式如下：

- 购买；
- 制造/编码；
- 重用。

这三种方式在后面各节中分别论述。图 5.1-1 针对产品的各个层次和寿命周期所有阶段，给出开展产品实施执行过程中的输入、输出和活动。这些活动包括准备进行产品实施执行、购买/制造/重用产品、获取产品实施执行流程的工作产品。某些情况下，产品实施执行的方式可能不止这些（如制造印刷）。这样，相应的方式应根据需要应用。

1. 准备进行产品实施执行

不管选择什么实施执行方式，准备进行产品实施执行是关键的第一步。对于复杂项目，需要开发和归档产品实施执行的策略，以及详细的计划和技术规程。对于不太复杂的项目，需要根据项目复杂程度讨论、审批和归档相关的实施执行策略和计划。

文档、规范及其他输入同样需要评审，以确保其准备就绪，并达到适当的详细程度，可以针对产品的寿命周期相应完成所采用的实施执行方式。例如，如果采用自主制造产品的方式，需要评审设计规范，确保设计规范处在允许产品开发的待设计层次上。如果准备购买的产品是商业现货产品，需要检查供货商的产品规范，确保其充分描述详细到产品系列中单件产品的制造/模型特征。

最后，还需要评审负责产品实施执行人员的可用性和技能，以及所有需要的原材料、辅

助产品或特殊服务的可用性。此时应当对开展这项工作所需的人员进行专门培训，使他们能够完成任务。

2. 产品的购买、制造和重用

1) 购买的产品

第一种情况，从商户或供货商处购买目标产品。在需求开发阶段生成产品设计/购买规范，并作为实施执行流程的输入。技术团队需要评审这些规范，确保它们适合采用签订合同或认购订单的形式。其包括起草合同、工作陈述、投标指南、认购订单或其他购买形式。政府部门与承包商的职责应当写入系统工程管理计划中。例如，其中需定义 NASA 是否期望供货商提供经过完全验证与确认的产品，是否由 NASA 技术团队负责此项工作。技术团队与采办团队协同工作，确保合同的工作陈述或认购订单精确，确保向供货商要求相应文档、合格证书，或提出其他特殊要求。

对于合同形式的购买，面对众多供货商的投标，技术团队应与合同官员共同工作，参与技术信息的评审，以及在费用和进度约束下选择满足设计需求的最佳供货商。

购买的产品到货后，技术团队应协助检查交付的产品及其配套文档。技术团队应当确保交付的产品确实是所需要的产品，并且所有需要的文档（如源代码、操作手册、合格证书、安全信息或设计图纸）已经签收。

技术团队还应该确保为产品试验、运行、维护和退役处置提供支持的辅助产品已按照合同规定准备就绪或已经提交。

根据系统工程管理计划中规定的供货商策略、作用和责任，若选择由供货商做产品验证和确认，可能需要对此决定/分析进行评审。评审可以依据产品的复杂程度采取正式或者非正式形式进行。对于由供货商验证和确认的产品，在确保已获得该阶段所有工作产品的基础上，可以认为产品已经准备就绪，能够进入向较高层次或最终用户提交产品的产品交付流程。对于由技术团队验证和确认的产品，在确保已获得该阶段所有工作产品的基础上，可以认为产品做好了验证准备。

2) 自行制造/编码的产品

如果产品的策略是自主制造或编码，则技术团队应首先确保辅助产品准备就绪。其包括确保所有零部件可用、设计图完整充分、软件设计完成并通过评审、切割材料的机械设备可用、接口规范已经批准、操作人员已训练并胜任、技术规程/流程已就绪、软件人员已培训并胜任编码工作、试验工具已开发并可应用于产品试验、软件试验大纲已完成并准备开始生成模型。

随即产品开始按照特定需求、技术状态文档和适用标准进行制造或编码。在整个过程中，技术团队应当与质量管理部门合作，适当时与高层管理人员合作，对团队内部的进展与状态进行评审、检查和讨论。进展应归档在技术进度表内。可能需要使用同行评审、产品审核、元件试验、代码检查、仿真校验及其他技术确保制造或生产的产品已为验证流程做好准备。

3) 重用的产品

如果产品策略是重用已有产品，必须仔细确保产品确实对项目及其既定的用途和将使用的环境是可用的。这是用于选择产品自制/购买/重用策略的决策因素。

技术团队应当评审来自重用产品的可用技术文档，达到对重用产品的完全熟悉，确保其满足特定环境中的需求。应当收集所有辅助手册、设计图纸或其他可用的文档。

应当确定产品制造、编码、试验、分析、验证、确认和运送所需的所有支撑和辅助产品或基础结构设施。如果缺少这些产品或服务中的任何一项，应在推进到下一阶段之前完成开发或准备就绪。

在获得重用产品之前，可能需要制定特别协议，如保密协议。

重用产品通常要经过与购买产品或自研产品一样的验证与确认过程。只有当产品的前期验证与确认文档满足当前项目的验证与确认需求和文档需求，且文档证实产品根据相应需求与期望通过验证与确认，才可以考虑依靠前期的验证与确认，而无须进行新的验证与确认。产品重用所节省的不仅是减少试验，而且降低了产品试验失败和重复工作的可能性。

3. 获取工作产品

不管采取什么产品实施执行方式，必须获取自制/购买/重用流程的工作产品，包括设计图纸、设计文档、代码清单、模型描述、所用技术规程、操作手册、维护手册或其他相应的文档。

5.1.1.3 输出

- **用于验证的目标产品：**除非由供货商进行验证，应当为验证流程提供适合寿命周期阶段的自制/自编、购买或重用的目标产品。目标产品的形式与寿命周期阶段，以及产品所处系统层次结构的位置相关（目标产品的形式可能是硬件、软件、模型、原型、试样及一次性或批量生产的物品）。
- **目标产品文档和手册：**相应文档与目标产品共同提交到验证流程和技术数据管理流程。文档可能包括相应的设计图纸、操作手册、用户手册、维护手册或培训手册；还包括控制基线文档（技术状态控制基线、规范、利益相关者期望）、合格证明或供货商的其他文档。

下述活动完成后整个流程完成：

- 目标产品已生产、购买或已获得重用模块；
- 目标产品已评审、检查并做好验证准备；
- 产品自制/购买/重用中形成的技术规程、决策、假设、异常及纠正行动、经验总结等都已归档备查。

5.1.2 产品实施执行指南

5.1.2.1 购买现货产品

现货产品是已有品牌的硬件/软件，通常有若干来源，包括商业的、军事的或 NASA 工程中形成的。在购买现货产品时需要特别注意其所使用的空间环境。多数现货产品是为在像地球这样的良性环境中使用而开发的，可能并不适应恶劣的空间环境，如真空、辐射、极端温差、极强的光照条件、失重、原子态氧、缺乏对流冷却、起飞时强振动和极大加速度、冲击载荷等。

购买现货产品时，仍要生成和管理相应需求。需要调查可用的现货产品并评价它们满足需求的程度。能够满足所有需求的产品是最佳候选产品。如果没有候选产品满足所有需求，需要进行权衡研究，确定是否可以放松或放弃需求条件，现货产品是否经修改可以满足条件，或是否应当选择自制和重用。

选择购买现货产品需要考虑的附加因素如下：

- 产品品质的一致性；
- 是否是关键性应用；
- 产品需要修改的工作量及执行人员；
- 是否有充分的可用文档；
- 产品的控制权、使用权、所有权、担保及许可；
- 供货商/供应商未来对产品的服务保障；
- 项目需要对产品进行的额外确认工作；
- 产品用户团队发现缺陷时的保密协定。

5.1.2.2 品质一致性

品质一致性是指在分部件制造系统时，初始制造商的品质与可靠性水平，由以下指标衡量：（1）服务时间；（2）服务机构数量；（3）平均故障间隔时间；（4）使用周期数。高品质一致性来自初始供应商，为绝大多数原始设备、设计、性能及制造特征提供维护。低品质一致性通常如下：（1）不是由初始制造者供货；（2）缺乏重大试验与使用经验；（3）原始设备、设计、性能及制造特征等关键方面出现变更。评估商业现货产品品质一致性的重要因素是确保产品的应用切实与期望应用相关。地面应用中的高品质一致性产品在空间环境中可能出现低品质一致性。

品质一致性评审的重点是证实组件在当前应用中的适用性。评估不仅需要考虑（硬件和软件）技术接口与性能，还需要考虑元件前期被证明合格时的环境，包括电磁兼容性、辐射和污染。部件的设计与质量需求的兼容性也必须评估。通过更改使得产品组件能够服从需求，或通过针对可接受的偏差做出正式的免责声明/允偏声明，来识别、处理和归档所有的非一致性。品质一致性评审通常紧接在合同签订之后进行。

在评审产品适用性时，重要的是考虑当前应用的性质。“灾难性”应用是指故障导致人员与飞行器损失。“关键性”应用是指故障导致使命任务失败。在这些应用中，需要采取预防措施，包括确保产品不会在其性能与环境许可范围的临界应用。在初步设计评审和关键设计评审过程中必须由专家严格审查把关，确保产品应用的适当性。

可能需要对现货产品进行修改，使之适用于 NASA 应用。这可能影响产品的品质一致性，因此，被修改的产品应看做新的设计。如果产品由 NASA 而非制造商修改，邀请供应商参与对产品修改的评审是有益的。NASA 的内部修改也可能需要从供应商处购买额外文档，如图纸、代码或其他相关设计与试验的描述。

关于现货产品的附加信息及推荐的试验与分析需求，参见具有 JSC EA-WI-016 或 MSFC MWI 8060.1 双编号的《飞行硬件开发中现货硬件的应用》，以及 G-118-2006e《AIAA 关键使命任务系统中商用现货产品软件组件的应用管理指南》。

5.2 产品集成

产品集成制造完成系统结构，是系统工程引擎的产品实现流程之一。在此流程中，较低层次产品被组装成较高层次的产品，并检验集成产品以确保其发挥正常功能。该流程位于产品实施执行流程和验证确认流程之间，这些流程共同完成将低层产品实现为高层目标产品。

产品集成流程的目的是由较低层次的产品或子系统（如产品单元、元件、组件、子系统或是操作任务）系统地组装成较高层次的产品；确保集成产品完成相应的功能；提交产品。系统层次结构的各层皆需要进行产品集成。与产品集成相关的活动贯穿产品的寿命周期。其中包括所有递进的步骤，如与产品层次相应的试验，这是完成产品组装与进行顶层试验所需要的。产品集成流程通常包括分析与仿真（如各类原型），并经常以此开始，然后通过现实中功能性的不断增加来推进流程，直至得到最终产品。在这些不断的构建过程中，需要根据评价流程中获取的知识进行原型的构建、评价、改进和重构。物理样机与虚拟样机的相对程度依赖于设计工具的功能、产品的复杂度及相应的风险。以这种方式集成的产品，通过产品验证和确认的可能性很高。对于某些产品，产品的最后集成可能发生在产品被部署到其确定的运行使用场地时。如果在产品验证和确认试验阶段有任何的不相容问题出现，它们必须逐个解决。

产品集成流程不仅应用于硬件和软件系统中，而且应用于面向服务的解决方案、需求、规范、计划和概念中。产品集成的终极目的是确保系统单元形成整体功能。

5.2.1 流程描述

图 5.2-1 所示的是产品集成流程提供典型的流程图，给出产品集成所关心的典型输入、活动及输出。产品集成流程的活动被简化地呈现为行动及行动对象。

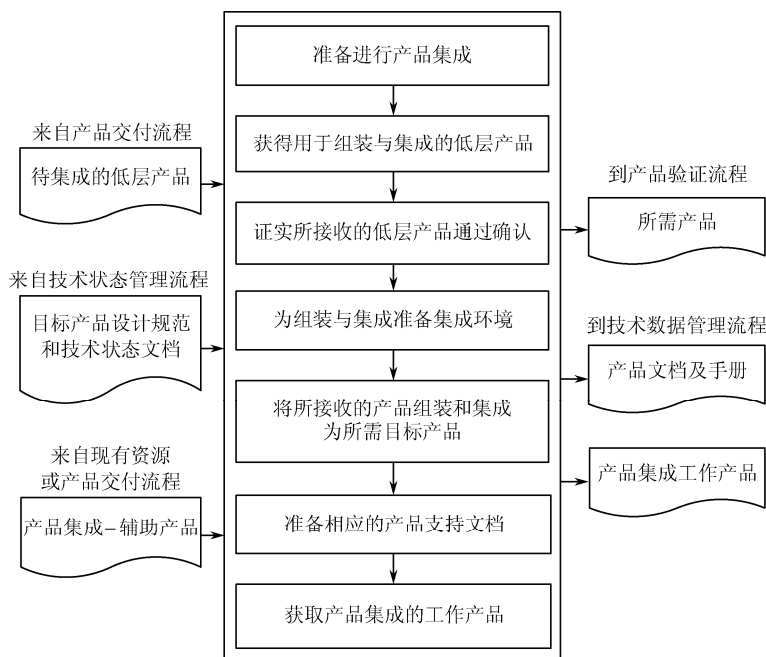


图 5.2-1 产品集成流程

5.2.1.1 输入

产品集成并不是设计与制造阶段结束时的一次性工作，而可能进行多次，该工作不仅涉及低层产品的集成，还涉及集成操作。必须制定和归档集成计划。附录 H 中给出集成计划的实例概述。产品集成递进执行一个递归流程：组装低层产品，执行集成操作，通过试验、检

查、分析或演示验证对组装进行评估，然后集成更高层次的产品及相关操作。产品集成计划应当在寿命周期的概念论证阶段启动。为了对支持产品集成的不同层次集成产品或集成操作的内部与外部接口进行有效管理，需要完成的基本任务如下：

- 定义接口。
- 辨识（物理的、电子的、机械的等）接口特征。
- 应用项目归档和审批流程来确保所有定义接口的兼容性。
- 在设计、构建和执行等过程中严格控制接口流程。
- 明确待组装与集成的低层次产品（来自产品交付流程）。
- 明确能够显示待集成产品完整技术状态的组装图或其他文档、部件清单、组装说明书（如紧固件的扭矩需求）。
- 以满足相关产品寿命周期阶段成功准则的适当形式，辨识目标产品、设计定义的特定需求（规范）、可用工作分解结构模型的技术状态文档，包括接口规范（来自技术状态管理流程）。
- 识别产品集成的辅助产品（来自于已有资源或是辅助产品实现的产品交付流程）。

5.2.1.2 流程活动

本节讲述产品集成流程直到顶层的实施方法，包括支撑该流程所需的活动。项目的全寿命周期中都将遵循该方法。

支持产品集成流程的典型活动如下所述。

- 准备进行产品集成：
 - 准备产品集成策略、详细的集成计划，以及集成的顺序和技术规程。
 - 确定产品技术状态文档是否足够执行与相关产品寿命周期阶段、产品在系统结构中所处的位置，以及管理的阶段成功准则等相应的产品集成流程。
- 获得用于组装和集成所需产品的低层产品。
- 证实所获得的用于组装和集成的低层产品已通过产品确认，证明单个产品满足协议中规定的利益相关者期望，包括接口需求。
- 准备用于进行产品组装和集成的集成环境，包括准备评估用于集成的辅助产品及为产品集成分配的劳动力。
- 根据特定的需求、技术状态文档、接口需求、实用标准，以及相应的集成顺序和技术规程将所获得的低层产品组装集成为所需的目标产品。
- 执行功能测试，确保组装的产品做好进入验证试验和集成到上一层次的准备。
- 准备相应的产品支持文档，如执行产品确认与产品验证的特殊技术规程。
- 获取在执行产品集成流程活动时产生的工作产品和相关信息。

5.2.1.3 输出

产品集成流程的典型输出及该流程产品的去向如下：

- 适应于相关产品寿命周期阶段，并满足阶段成功准则（对于产品验证流程）的集成产品。
- 适应于满足寿命周期阶段成功准则的文档和手册，包括正在集成产品的描述及其操作和维护手册（对于技术数据管理流程）。

- 工作产品，包括产品集成活动的报告、记录和非提交结果（用于支持技术数据管理流程）、集成策略文档、组装/检查区域图纸、选择组装的系统/组件顺序和依据，接口管理文档、人员需求、特殊处理需求、系统文档、运输规划、试验装备和动因需求、仿真器需求、对硬件与软件局限性的标识等。

5.2.2 产品集成指南

5.2.2.1 集成策略

集成策略及相应支撑文档的开发是为了确定组成系统的各类组件接收、组装和激活顺序。集成策略应当采用商业与技术手段确保组装、激活和装载顺序能使成本和组装困难最小化。系统规模越大越复杂或系统单元越精密，找出适当顺序就显得越重要，因为微小的变化可能对项目结果产生很大的影响。

最优组装顺序自底向上建立，如组件装配形成子单元、单元和子系统，其中每个在进行更高层组装之前必须经过检查。该顺序包括建立或配备组装设施（如升降机、起重机、夹具、测试设备、输入/输出、动力连接）所需的所有工作。最优顺序一旦确定，必须定期评审确保生产和交付进度的变化不会对顺序产生负面影响，并且不会影响早期决策中考虑的因素。

5.2.2.2 与产品实施执行的关系

如前所述，产品实施执行是将开发的产品计划、设计、分析、需求及设计图纸实现为真实产品。产品集成侧重于接口的控制及达成满足需求的正确产品的确认与验证。产品集成可以看做正式投产或阶段性的提交。产品集成是将新的和已有的产品整合在一起并确保在没有干扰和困难的情况下整合得到完整产品。如果出现问题，产品集成流程将此意外情况记录归档，用于评价并决定产品是否可以进入实施/运行使用阶段。

集成发生在项目寿命周期每个阶段。在规划论证阶段，分解的需求需要集成为完整的系统以验证是否有遗漏和冗余。在实施运行阶段，设计与硬件需要集成为完整系统，以验证其满足需求且没有冗余和遗漏。

系统工程强调递归、迭代和集成特性，表明产品集成活动不仅用在项目初始计划阶段即确定全寿命周期所有阶段集成，而且递归应用于贯穿全寿命周期阶段的通过系统工程引擎执行的项目产品向下分解和向上集成中。这就确保在需求、设计构思等发生变化（通常是反映来自利益相关者或分析、建模与测试结果的更新）的情况下，可以对项目进行适当的修正。完成此修正需要通过系统工程引擎进行重新评估，使得产品集成活动的所有方面适当更新。最终使产品满足项目批准的修正，减少在项目后续阶段中修正工作的时间成本耗费。

5.2.2.3 产品/接口集成支持

有若干流程支持产品和接口的集成。这些流程或支持对产品和接口的集成，或支持对集成产品是否满足项目需要的确认。

支持产品和接口集成并且在整个产品集成过程中应当说明的流程和产品典型示例如下：需求文档、需求评审、设计评审、设计图纸和规范、集成和测试计划、硬件技术状态控制文档、品质保证记录、接口控制需求/文档、运行使用构想文档、验证需求文档、验证报告/分析、NASA 标准、军用标准、工业标准、最佳实践和经验教训。

5.2.2.4 设计方案的产品集成

本节论述与选定设计方案相关的更具体的产品集成实施。

通常系统/产品的设计是子系统与组件组合的过程。这对复杂硬件/软件系统相对明显。对许多面向服务的解决方案也如此。例如，提供个人与互联网连接的方案，涉及到硬件、软件和通信接口。系统集成的目的是确保这些单元的组合达到预期结果（如按期待正常工作）。因此，内部接口和外部接口必须在设计中考虑并且在生产之前进行评价。

对各层产品集成的验证有许多类型的试验需求。合格试验和验收试验是对集成中产品进行各类试验的两个例子。另一种试验类型是所开发的构件在真实和模拟的任务剖面环境内试验，以揭示设计缺陷并为故障模式和控制机制提供工程技术信息，这是计划好的试验流程，对产品设计 and 目标产品集成非常重要。如果构件开发完成，该试验可提供早期发现产品问题的能力，否则，只能在产品集成的后期阶段才能发现问题，从而造成修正工作的额外成本。对于大型复杂系统/产品，集成/验证工作都使用原型进行。

5.2.2.5 接口管理

接口管理的目标是在所有相互关联系统单元间达到功能上与物理上的兼容性。接口管理在 6.3 节有详细的定义。接口是功能区域之间的边界。接口可以是认知的、外部的、内部的、功能性和物理性的。接口可以出现在系统内部或系统与另一个系统之间，可以具有功能性或物理性（如机械、电子）。接口需求在接口需求文档中描述。生成接口需求文档时应当注意定义接口需求并避免指定设计方案。接口控制文档的最终形式描述包含在接口需求文档中需求的实现细节。接口控制计划描述接口需求文档与接口控制文档的管理流程。该计划提供辨识并解决接口不兼容性的方法，并确定接口设计变更的影响。

5.2.2.6 兼容性分析

在项目寿命周期中，必须维护不同单元的兼容性与可达性。接口定义的兼容性分析说明接口及其追溯记录的完整性。当出现变更时，必须结合相关文档安排控制接口设计的权威方法，从而避免出现硬件和软件集成到系统中时，不能实现其在系统中预定功能的情况。确保系统组成部分能够协调工作是一项复杂的任务，涉及技术团队、利益相关者、承包商等，以及从初始概念定义阶段结束到运行与保障阶段的工程项目管理。物理集成在阶段 D 完成。在系统相应的层次，系统组成部分必须经过试验、组装和/或集成，并再次试验。系统工程师的作用包括执行委派的管理任务，如技术状态控制及监督集成、验证和确认流程。

5.2.2.7 接口管理任务

接口管理任务在产品开发早期开始，此时接口需求受所有工程学科和可引用的实用接口标准影响。接口管理任务通过设计和检验进行。在设计中，重点是确保接口规范得到归档和沟通。在系统单元检验中，针对组装前及组装后的技术状态，重点是验证接口的实现。在整个产品集成流程的活动中，接口控制基线受到控制以确保系统单元的设计变更对与其有接口关系的其他系统单元影响最小。在试验和其他相关验证与确认活动中，对集成为系统或子系统的多个系统单元都应进行检验。以下部分是关于这些任务的更详细讨论。

1. 定义接口

大部分集成中的问题出自接口的不明确或不可控。因此，应在开发工作中尽早明确系统和子系统接口规范。接口规范需说明接口有关逻辑、物理、电子、机械、人文和环境方面相应的参数。系统中的子系统开发首先考虑系统内部接口的设计。接口使用前期开发成果或根据与确定的学科和技术相应的接口标准进行开发。迫不得已情况下才构造新的接口。接口规范按照接口需求进行验证。典型产品包括接口描述、接口控制文档、接口需求和接口规范。

2. 验证接口

在接口验证中，系统工程师必须确保系统或子系统中每个单元的接口是开发者可控和已知的。另外，当需要对接口进行变更时，至少要评估接口变更对其他有接口关系单元的影响，并与受影响单元的开发人员沟通。即使受影响单元的开发人员是决定变更组织中的成员，这种变更还是需要能够容易实现，从而保证接口的当前状态被所有成员知晓。典型的产品包括接口控制文档和意外情况报告。

如果仿真器的局限性被明确描述，并且满足接口验证的运行环境特征和行为需求，使用仿真器进行硬件与软件接口验证是可接受的。在集成计划中应该专门说明仿真器的使用范围。

3. 检查并确认系统与子系统所需单元收悉

在按照预定的设计组装系统之前需要确认收悉并检查每个系统或子系统单元的状态。需要检查单元的数量、有无明显瑕疵，以及单元描述与单元需求的一致性。典型产品包括单元验收文档、交付收据和经核实的包装清单。

4. 验证系统与子系统单元

系统与子系统单元的验证可以证实所开发或购买的系统单元的设计特征满足相应需求。这样做是确保系统/子系统单元在预定的环境中正常发挥作用，包括作为其他环境中现货产品的单元。这种验证可能是试验（如回归试验作为工具或子系统/单元结合进系统）、检查、分析（关于不足或满足的报告）和演示验证，可以由组装或生产系统/子系统单元的组织执行。有必要给出相应的方法能够从“不合格”单元中判断实际“通过”验证的单元。典型产品包括经验证的系统特征和例外情况报告。

5. 验证单元接口

系统单元接口的验证确保单元在集成到系统之前服从接口规范。意图是确保系统与子系统每个单元的接口根据相应的接口规范得到验证。这种验证可能是试验、检查、分析或演示验证，可以由进行系统或子系统组装的组织或其他组织执行。典型产品包括经验证的系统单元接口、测试报告及例外情况报告。

6. 集成与验证

系统单元的组装应当根据制定的集成策略进行。由此确保根据计划的策略进行系统单元到更大更复杂系统的组装。为了确保集成能够圆满完成，需要对集成后系统的接口进行验证。典型产品包括集成报告、例外情况报告及集成系统。

5.3 产品验证

产品验证流程是对已实现的目标产品展开验证与确认流程的第一步。在系统工程通用技术流程的背景下，已实现产品由产品实施执行流程或产品集成流程以满足相应寿命周期成功准则的适当形式提供。流程的实现是通过验证和确认行动，将实现的产品交付系统结构更高层次或交付客户使用。简言之，产品验证流程回答如下关键问题：目标产品是否被正确地实现？而产品确认流程相应回答如下关键问题：所实现的是否为正确的目标产品？

验证流程证明通过系统结构中的各种系统模型所实现的产品遵从待构建产品的需求（对软件单元）或待实现规范和设计描述文档（对硬件单元、人工技术规程，或硬件、软件及人工技术规程的组合产品）。

产品验证与产品确认辨析

从流程的角度来看，产品验证与确认在性质上很相似，但是它们的目标却根本不同。

证实所实现的产品遵从其规范和设计描述文档（此即验证含义）是十分必要的。这些规范和文档确立产品的技术状态控制基线，这个控制基线在后续阶段中可能会修改。如果没有控制基线验证和适当的技术状态控制，这些后续的修改可能代价巨大并带来产品性能上的较大问题。然而，从客户的角度看，关注点是所提供的目标产品能否在其使用环境中按照客户的期望工作（此即确认含义）。如果通过分析能保证产品的成效，可以同时进行验证与确认联合试验，从而减少单独进行产品确认试验的花费。

产品验证流程的结果证实，不论通过实施执行还是通过集成得到的已实现产品，都遵从其特定需求，即证实目标产品通过验证。本节讨论验证输入、流程的活动、输出结果及潜在缺陷。

验证试验与确认试验辨析

- **验证试验：**验证试验针对的是经批准的需求集（如系统需求文档），试验可以在产品寿命周期的不同阶段执行。

验证试验如下：

- 任何用于辅助产品或产品单元开发与定型、辅助制造或保障流程的试验。
- 任何用于验证技术进步状态，验证设计风险最小化，证实达到合同要求的技术性能，证明初步确认试验已准备就绪的工程技术试验。验证试验使用仪器设备及评价指标，通常由工程师、技术人员、操作维护试验人员在有利于进行失效分析的受控环境中完成。
- **确认试验：**确认试验针对的是运行使用构想文档。确认试验在各个目标产品的真实环境或模拟环境中进行，确定典型用户执行的使命任务应用中产品的有效性与适用性，并评估试验结果。试验是适用于验证与确认的详细定量方法。当然，试验需要确认待生产和部署的目标产品的有效性。

5.3.1 流程描述

图 5.3-1 给出产品验证流程的典型流程图，并确定在产品验证中所关心的典型输入、活动及输出。

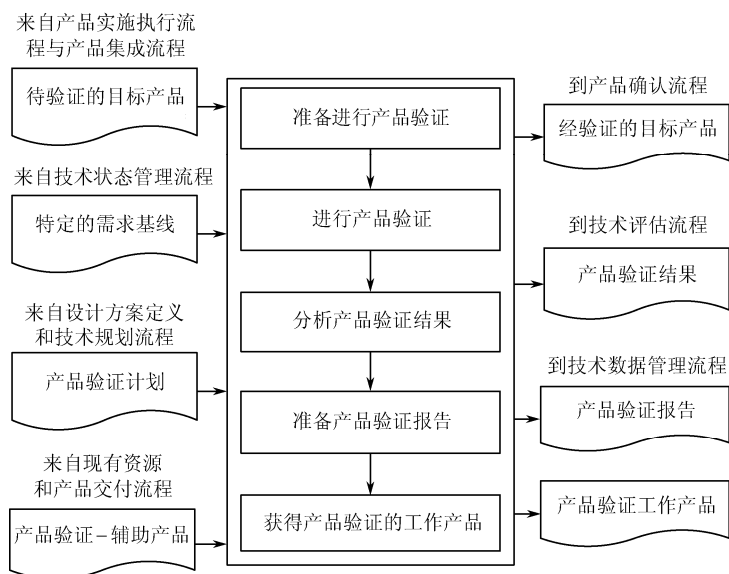


图 5.3-1 产品验证流程

5.3.1.1 输入

产品验证流程的关键输入包括待验证产品、验证计划、特定需求控制基线及所有执行产品验证流程的辅助产品（包括运行使用构想、使命任务需求与目标、需求和规范、接口控制图、试验标准及政策、NASA 总局标准及政策）。

5.3.1.2 流程活动

产品验证流程分为 5 个主要步骤：（1）验证计划（准备实施验证的计划）；（2）验证准备（准备进行验证）；（3）执行验证（进行产品验证）；（4）分析验证结果；（5）获得验证工作产品。

产品验证流程的目标是获得必要的证据以确保系统结构中从底层到顶层的目标产品都遵从特定需求（规范和描述文档），不论产品是由产品实施执行流程还是由产品集成流程得到。

产品验证通常由生产目标产品的开发者在最终用户与客户的参与下实施。产品验证证实已实现产品遵从其用于制造或组装集成目标产品的特定需求（规范与描述文档），不论该产品来自于产品实施流程还是来自于产品集成流程。通常验证试验涉及系统的开发者及用户。同时，客户和质量保证人员在验证计划的制定与活动的执行中同样起着重要的作用。

1. 产品验证计划

为产品验证制定计划是重要的第一步。根据相关规范和产品形式，验证方式（如分析、演示验证、检查和试验）的确立应当考虑产品寿命周期阶段、成本、进度、资源及产品在系统结构中的位置。验证计划应当针对特定技术规程、约束、成功准则或其他验证需求评审（基于设计方案输出、验证技术规划流程输出）。验证计划概要实例参见附录 I。

试验的类型

有许多类型的试验可用于目标产品的验证。可以考虑的试验类型如下：

- | | | |
|------------|------------------|--------------|
| • 气动力学试验； | • 验收试验； | • 声学试验； |
| • 老化试验； | • 特性试验； | • 组件试验； |
| • 坠落试验； | • 电磁兼容性试验； | • 电磁干扰试验； |
| • 环境试验； | • 过载试验； | • 通过/不通过试验； |
| • 高/低压限试验； | • 人因工程/人在回路试验试验； | • 集成试验； |
| • 漏损率试验； | • 寿命/周期试验； | • 制造/随机缺陷试验； |
| • 标称试验； | • 非标称试验； | • 操作性试验； |
| • 参数试验； | • 性能试验； | • 压力循环试验； |
| • 压力极限试验； | • 合格检验试验； | • 结构功能试验； |
| • 安全检查试验； | • 系统试验； | • 热循环试验； |
| • 发热极限试验； | • 热真空试验； | • 振动。 |

2. 验证计划及相关方法

准备验证计划的任务包括根据寿命周期阶段、产品在系统层次结构中所处的位置、产品的使用形式、验证个体特定需求的相对成本等，确定执行验证的类型。验证类型包括分析、检查、演示验证和试验或这四种方法的组合。验证计划通常在详细技术层面撰写，在自底向上的产品实现过程中起中枢作用。

注：验证计划与项目的系统工程管理计划相一致是绝对重要的。

验证流程针对不同形式的产品，在项目的全寿命周期中递归执行。产品形式如下：

- 仿真产品（算法模型、虚拟现实仿真器）。
- 样机（木质样品、硬试样或软试样）。
- 概念描述（纸质报告）。
- 原型（具有部分功能的产品）。
- 工程件（实现全部功能却可能形式或尺寸不同）。
- 设计验证试验件（相同形式、尺寸和功能，但不包含飞行件）。
- 合格检验件（与飞行件一致，但可能承受极端环境）。
- 飞行件（用于飞行的目标产品，包括原型飞行件）。

任何类型的产品可能处于以下状态：

- 生产的（构建、建造、制造或编码）。
- 重用的（内部未完全开发产品改造或现货产品）。
- 组装与集成的（低层次产品的组合）。

在进行产品验证之前应该建立进行产品验证的条件和环境，确定基于相关成功准则的产品验证计划。需要应用决策分析流程帮助确定详细计划。

注：对目标产品的决定性官方验证应当针对受控件。通常，试图在原型系统上“买通”以“需要”形式陈述的需求是不能接受的；这种情况通常发生在受控件的合格验证、飞行验证或最终验证中。

应当准备基于所计划类型（如分析、检查、演示验证、试验）进行的验证技术规程。这些技术规程通常在项目寿命周期的设计阶段开发，并且随着设计的成熟而不断成熟。需要思考运行使用的应用想定以便开发所有可能的验证活动。

验证的类型

- **分析：**基于计算数据或系统结构低层次目标产品验证所得数据，应用数学建模与分析技术预测产品设计针对利益相关者的适用性。在没有产品原型、工程模型或是制作/组装/集成的产品时，通常使用分析方法。分析通常将建模与仿真作为分析工具。模型是现实的数学描述，而仿真是对模型进行的运行操作。
- **演示验证：**用来显示目标产品使用是否达到特定需求。它是证实产品性能的基本方式，因缺乏详细数据的收集而与试验不同。演示验证可能涉及物理模型或样机的使用，例如，“所有控制装置对于宇航员可达”的需求，可以通过宇航员在驾驶舱模型或模拟器中执行相关飞行任务来验证。演示验证也可由高素质人员，如试飞员在目标产品上实际操作，进行单项演示验证，证实极端条件下的系统性能，执行通常不期望宇航员完成的非正常操作。
- **检查：**对所实现的目标产品做外观检查。通常用来验证产品的物理设计特性或辨识特定制造者。例如，某项需求是在有红色标记的安全保险销上镌刻黑色钢印：“发射前移除”，对安全销钢印标记的外观检查就可以用于确定需求是否满足。
- **试验：**用于获得验证目标产品性能所需的详细数据，或为通过进一步分析检验验证性能提供充足的信息。试验可以针对目标产品、软试样、硬试样或原型进行。试验在受控的条件下在离散的时刻点上针对特定需求产生数据，并且是资源最密集的验证方式。正如俗语所云：“像飞行那样试验，像试验那样飞行。”见 5.3.2.5 节。

验证计划如下所述。

- 已选定的适应于显示和证明已实现产品服从其特定需求的验证类型。
- 产品验证技术规程清晰定义的基础：
 - 为每种验证类型选择的技术规程；
 - 每个技术规程的目的与目标；
 - 所有验证前和验证后的行动；
 - 判定技术规程执行成功或失败的准则。
- 已定义的执行产品验证技术规程所需要的相关验证环境，例如，设施、设备、工具、仿真环境、测量设备及气候条件。
- 适当时候，考虑到验证策略不能完全复制集成试验系统、技术状态和/或设定的运行环境，应输出基于批准的验证策略对项目风险事项的更新。合理依据、权衡空间、优化结果和方法含义写进新的或改进的风险陈述，并作为适应未来项目控制基线设计、试验和使用变更的参考。

注：验证计划在项目寿命周期早期的需求开发阶段开始着手制定（参见 4.2 节）。确定使用哪种验证方法应该作为需求开发阶段工作的一部分，计划未来的活动，在辨识验证的辅助产品时建立相应的特殊需求，确保技术陈述是可验证的需求。验证计划更新持续贯穿逻辑分解和设计方案开发，特别是在对所考虑事项进行设计评审和仿真时（参见 6.1 节）。

3. 产品验证准备

在产品验证准备中，要收集和证实特定需求（设计方案流程的输出）。需要获得待验证的产品（实施执行阶段和集成阶段的输出）及验证所需的辅助产品和保障资源（确认的需求和设计方案定义活动的产物）。验证准备的最终元素包括准备验证环境（如设施、设备、工具、

仿真环境、测量仪器、人员和气候条件)。环境需求的确定是必要的,必须仔细考虑这些需求的含义。

产品验证的准备成果如下:

- 已完成执行所计划验证的准备活动。
- 适当的特定需求集合和相关支持技术状态文档已经准备就绪。
- 按照验证计划与进度安排,进行验证所需要的物品/模型已准备就绪,并组装与集成在验证环境中。
- 进行验证所需要的相关资源已经按照验证计划与进度安排准备就绪。
- 验证环境已进行充足性、完整性、预备性和整体性评价。

注:根据验证的性质和工程项目所处的寿命周期阶段,通常需要进行某类评审来评估验证的预备性(随后的确认工作亦如此)。在寿命周期早期阶段,这种评审可非正式进行;而在后期阶段,则成为试验成熟度评审的正式内容。试验成熟度评审和其他技术评审是技术评估流程的活动。

对于多数项目,进行大量经启动/成功准则裁剪的试验成熟度评审,以评估试验范围、试验设施、受训试验人员、仪器仪表、集成场地、保障设备和其他辅助产品的成熟度和可用性。

同行评审作为补充评审可正式或非正式进行,以确保验证(及验证流程的结果)的成熟度。

4. 按计划执行产品验证

目标产品的实际验证活动按照计划和技术规程所阐明的进行,并遵从每个特定的验证需求。负责的工程师要确保验证技术规程得到遵守并按照计划执行,验证的辅助产品已经过准确的校验,相关数据按照所需的验证指标进行收集和归档。

需要对验证计划、验证环境和/或验证实施进行的修改,应借助决策分析流程做出决策。

按计划执行产品验证的成果如下:

- 获取验证结果并进行评价,能够表明验证目标已完成,从而证明产品得到验证;
- 确定已实现的目标产品是否(以寿命周期阶段的适当形式)满足其特定需求;
- 确定验证产品是否与验证环境充分集成,并且每个验证需求是否被适当地验证;
- 确定产品功能及与其全部性能相关的接口产品已被共同验证。

5. 分析产品验证结果

一旦完成验证活动,应收集和分析验证结果。这些数据用于分析质量、完整性、正确性、一致性、有效性。任何验证的异常、偏差或不符合条件情况需要识别和评审。

偏差、异常或者不符合条件情况必须为后续行动和处理做记录并报告。验证结果应当记录在技术需求定义流程中或记录在为追踪每个验证需求一致性的机制下开发的需求一致性矩阵中。

如果即使在不严格的验证执行、设计或条件下仍引起异常,则可能需要系统设计与产品实现流程活动解决这些异常。如果异常是由严格的验证执行、设计或条件引起的,且这些异常的缓解导致产品的变更,则可能需要重新计划和执行验证流程。

分析产品验证结果的成果如下:

- 辨识出目标产品的偏差、异常、不符合条件情况。
- 为解决上述偏差、异常、不符合条件情况(进行非低劣验证引起的问题),适当的重

新计划、重新定义需求、重新设计和重新验证已经完成。

- 产品偏差、差异或不符合条件情况被接受并处理。
- 按照需要生成的差异及相应修正行动报告。
- 完成验证报告。

6. 流程重组

基于对验证结果的分析，可能需要重新实现用于验证的目标产品，或基于所发现缺陷的位置和类型对组装和集成到验证产品的目标产品进行验证流程重组。

流程重组可能需要重新应用系统设计流程（包括利益相关者的期望定义、技术需求定义、逻辑分解及设计方案定义）。

7. 验证中出现的不足

验证试验结果若不能令人满意可能有若干原因。一方面是验证流程执行不力（如没有遵守技术规程、设备没有校准、不合适的验证环境条件或未能控制与特定需求验证无关的其他因素）。另一方面是所用的已实现目标产品没有正确实现。

重组系统设计流程所需的工作如下：

- 对构成发现缺陷（即未满足验证需求）产品的系统结构中低层次产品重组系统工程流程。
- 重新执行产品验证流程。

注：需求不符和差异情况报告可能直接与技术风险管理流程相关。依据需求不符的性质，相关报告可能需要经过材料评审委员会和技术状态控制委员会（通常包括风险管理分委员会）的审批。

8. 通过验证却没有通过确认怎么办？

许多系统通过了验证，却未通过确认流程的某个关键阶段，延迟了开发并产生大量重复工作，而且可能不被利益相关者承认。防止确认不成功的关键是在项目的早期阶段开发可靠的运行使用构想（并在需求开发与设计阶段对其进行提炼）。与利益相关者进行沟通有助于确定在设计和实现目标产品时必须理解的运行使用想定与关键需求。产品确认可能失败，必须面对现实重新设计。需要对先前理解的需求集、已有的设计、运行使用想定和支撑材料进行评审，并与客户、其他利益相关者和/或最终用户沟通达成妥协，确定修正和解决当前状况可以开展的工作。但是这样会增加整个项目的时间和成本，甚至可能导致项目失败或取消。

9. 获取产品验证的工作产品

验证的工作产品（输入到技术数据管理流程）有多种形式，包含许多信息源。验证结果和数据的获取与归档是产品验证流程中非常重要的一步，却经常重视不够。

需要获取验证结果、异常和采取的修正行动，以及产品验证流程的所有相关结果（相关决策、决策的依据、假设和总结的经验）。

获取验证工作产品的成果如下：

- 验证工作产品已记录，如验证类型、技术规程、环境、结果、决策、假设、修正行动、总结的经验。

- 偏差、异常、条件不符情况，包括采取的相应解决行动已识别和归档。
- 已实现目标产品满足或不满足特定需求的证明已归档。
- 形成验证报告，内容包括以下几个方面。
 - 记录试验/验证的结果/数据；
 - 使用的特定需求集的版本；
 - 已验证产品的版本；
 - 所应用工具、数据和设备的版本或标准；
 - 包括成功或失败声明的每个验证的结果；
 - 期望与实际的差异。

5.3.1.3 输出

产品验证流程的关键输出如下：

- 差异报告及确定的修正行动；
- 用于确认或集成的已验证产品；
- 验证报告及需求一致性文档的更新（包括验证计划、验证技术规程、验证指标、验证结果及分析，以及试验/演示验证/检查/分析记录）。

成功准则如下：

- 归档每个服从（或可能偏离）所关注的系统需求的客观证据；
- 所有偏差报告都已处理。产品验证流程在所有偏差报告处理完毕（即所有发现的错误处理完毕）后才能认定为完成。

5.3.2 产品验证指南

5.3.2.1 验证程序

验证程序应根据其支持的项目剪裁。项目负责人/系统工程师必须与验证工程师合作，开发验证程序的概念。在开发验证程序概念及具体的验证程序时，有许多因素需要考虑。这些因素包括如下所述。

- 项目特别是飞行项目的类型。验证方法安排取决于如下情况：
 - 飞行器类型（如试验、有效载荷或者运载火箭）。
 - NASA 有效载荷分类（NPR 8705.4 《NASA 有效载荷的风险分类》）。验证指南期望作为建立正式试验程序的起点，基于 NPR 8705.4 的“A-D”有效载荷分类的特定项目可根据需要对试验程序进行裁剪。
 - 项目成本与进度含义。验证活动是影响项目成本与进度的重要因素，应该在开发验证程序的早期考虑这些活动的含义。应当进行支持有关验证方法和需求，以及支持验证的设施类型及场所决策的权衡研究。例如，可能需要为决定在集中设施上还是分布在若干不同地点的设施上进行试验做权衡研究。
 - 风险含义。在验证程序开发中，必须考虑风险管理。定性的风险评估与定量的风险分析（如失效模式及影响分析 FMECA）通常辨识那些能够通过附加试验而减缓的新的风险关注点，这样将扩大验证活动的有效范围。其他风险评估对权衡研究的作用

用在于确定应用的验证方法及其应用时机。例如，需要做的权衡是直接进行模型试验，还是通过低成本而可能发现问题较少的分析以先行确定模型特征再试验。项目负责人/系统工程师必须决定项目在成本与进度方面可接受的风险水平。

- 验证设施/场站和运输工具的可用性，（需要时）能够在不同场站之间传输物品。这需要与综合后勤保障工程师协调完成。
- 采办策略（即确定自主开发或合同订购）。通常，NASA 试验中心可以根据项目的任务书制定承包商的验证流程。
- 设计的继承性及软/硬件的重用性。

5.3.2.2 寿命周期中的验证

完成验证的类型与寿命周期阶段及目标产品在系统结构中的位置相关。在自底向上的实现流程中，目标产品在交付到更高层次前必须验证与确认（见图 5.3-2）。

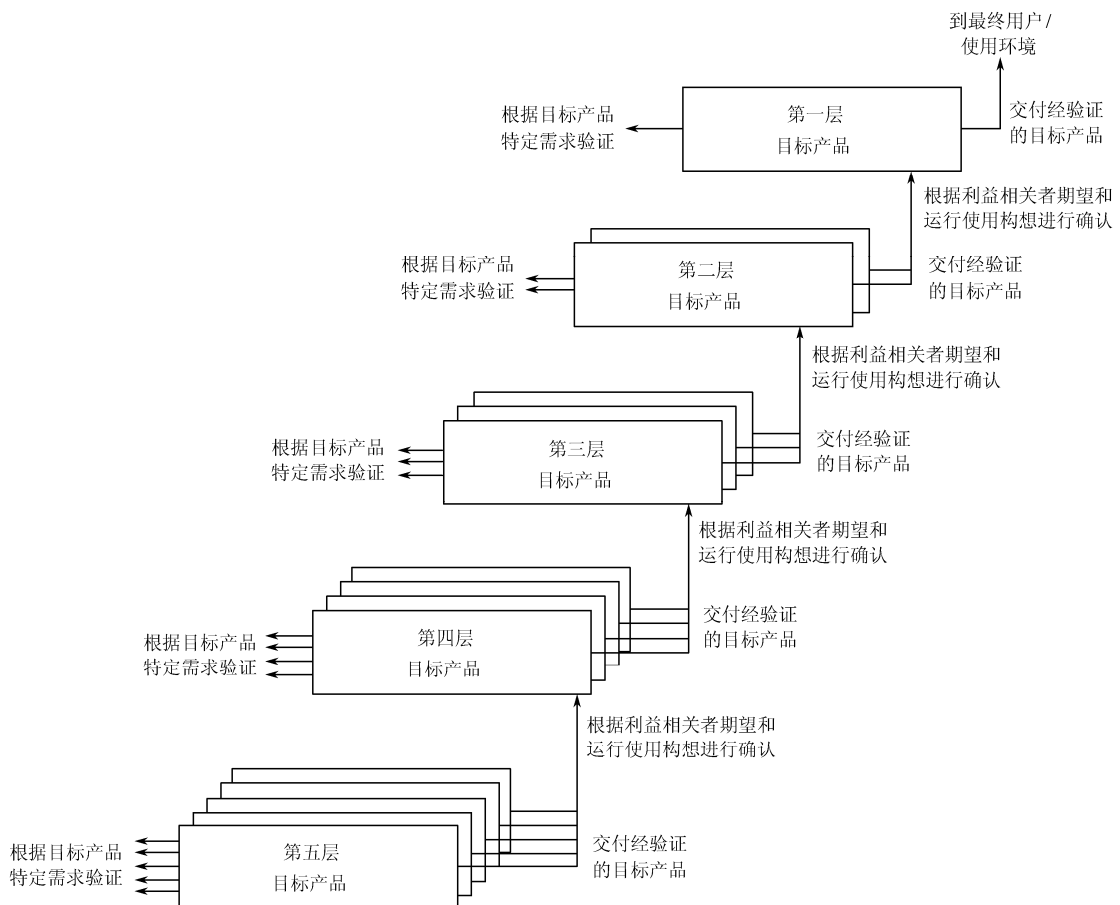


图 5.3-2 自底向上的产品实现流程

尽管在这里被描述为不同的流程，在实施时某些验证与确认事件有相当多的重叠。

1. 产品验证中的质量保证

即使有完美的产品设计、硬件制造、软件编码和试验，项目仍将遇到自然和人员方面的异常。系统工程师必须有信心，实际系统的确是根据其功能、性能和设计需求生产并交付的。

质量保证为项目负责人/系统工程师提供项目寿命周期中针对生产的产品和使用的流程进行的独立评估。此时质量保证工程师通常扮演系统工程师的眼睛和耳朵的角色。

质量保证工程师通常监督需求不符及问题/失败报告的解决方案与处理过程；验证系统技术状态遵从在关键设计评审中批准的建造（编码）文档；收集并维护用于后续失效分析的质量保证数据。质量保证工程师也参与关于可能导致产品系统质量的设计、材料、工艺、制造及验证过程方面问题的重要评审（主要是系统需求评审、初步设计评审、关键设计评审和飞行准备状态评审）。

项目负责人/系统工程师必须与质量保证工程师协同开发为支持项目而裁剪的质量保证程序（质量保证活动的范围、职责和时限）。部分质量保证程序确保验证需求适当和明确，特别是在试验环境、试验技术状态、成功/失败准则方面，同时监控合格试验和验收试验以确保其服从验证需求和试验技术规程，确保试验数据的正确性和完整性。

2. 技术状态验证

技术状态验证是对所得到的产品（如硬件与软件产品）符合控制基线确定的设计进行验证，以及对控制基线文档新颖性和精确性的验证流程。技术状态验证通过两种类型的控制通道活动完成：审核与技术评审。

3. 合格性验证

合格性验证阶段的活动在完成飞行/运行用硬件的设计开发之后启动，这些活动包括分析与试验，以确保飞行/运行用硬件（和软件）在预定的环境条件下满足其功能与性能需求。在这一阶段，许多性能需求被验证，同时分析手段与模型随着试验数据积累而更新。合格性试验通常设计为使硬件面对最差的负载情况与工作环境强度，加上确定的余量水平。为确保硬件服从性能需求而执行的某些验证涉及振动/声学、压力极限、漏损率、热真空、热循环、电磁干扰和电磁兼容性、高压限和低压限、寿命/寿命周期。在危险分析报告中定义的安全需求可能也要在此验证试验中满足。

合格性验证通常发生在组件或子系统层次，但也可能发生在系统层次。若项目决定不制造专用的合格性验证用硬件，而使用飞行/运行用硬件自身，则称为“原型飞行”。此时，需要验证的需求比合格水平验证时少，而比验收水平验证时多。

合格性验证可以验证设计的稳固性。试验水平通常在期望的飞行/运行水平上设置一定余量，包括可能需要在验收试验中积累的最大循环数量。这些余量总体上设置为设计安全余量，应当注意不要设置试验层次，以免出现不切实际的失效模式。

4. 验收验证

验收阶段验证活动为飞行/运行用硬件和软件与其功能、性能和设计需求一致并准备就绪可以运送至发射场提供保障。验收阶段开始于对每个用于组装成飞行/运行用产品的单个组件或部件的验收，并持续到系统验收评审（参见 6.7.2.1 节）。

某些验证不能在飞行/运行用产品，特别是大型产品组装和集成后进行（可能因为此时不可达）。当此情况发生时，验证活动要在制造与集成过程中展开，称为“过程中”试验。在此情况下，验收试验与过程中试验同时开始，持续进行功能试验、环境试验、全系统兼容性试验。功能试验通常始于组件层并持续到系统层，与系统整体运行试验同时结束。

当飞行/运行用硬件不可用时，或其使用对特定试验不合适时，可能需要使用模拟器验证接口。试验中出现的异常在适当的报告系统中归档，在继续试验之前需制定相应的解决方案。

主要异常或不易处理的异常，可能需要系统工程师与设计人员、试验人员和其他组织合作形成解决方案。分析手段及模型随试验数据的积累适时得到确认与更新。验收验证针对工艺水平，而非设计水平。试验重点设置在产品层，可以发现源自部件、材料和工艺中的缺陷。这样，试验层次可在无额外余量的飞行/运行过程中预测。

5. 部署验证

该验证阶段的活动开始于发射前飞行/运行用产品到达发射场，在发射后结束。在这一阶段，飞行/运行用产品被测试并与运载器对接。运载的形式可能是航天飞机或其他运载火箭，或飞行/运行用产品本身是运载火箭的一部分。这一阶段的验证活动确保地面运输过程中系统没有遭受明显毁坏，可以按照要求完成相应功能。

如果系统单元是分别运送到发射场实施组装，通常需要对系统及系统接口进行试验。如果系统需要与运载器集成，与运载器的接口也必须验证。其他验证包括集成到运载火箭后进行验证和在发射台上进行验证，这些是为确保系统功能正常且处于合适的发射技术状态。对于可能在发射前和倒计时发生的可预见的紧急情况，需要开发应急验证方案和应急技术规程。应急验证方案和应急技术规程在某些紧急情况需要运载火箭或飞行/运行用产品从发射台回退到测试设施时非常关键。

6. 运行使用与退役处置验证

运行使用验证开始于阶段 E，提供系统在有关环境中发挥正常功能的保证。这些验证是通过系统的启动和运行完成的，而不是通过验证活动。在轨组装的系统必须进行接口验证，必须在全系统试验中功能正常。提供液体或气流的机械接口必须验证确保没有泄漏发生，且压力与流体速度在规定范围内环境系统必须验证。

退役处置验证保证所有系统产品和流程的安全解效和处置已经完成。退役处置验证活动开始于阶段 F 的适当时刻（即或按计划进行，或在提前失效或事故发生的早期进行），在已获取所有使命任务数据及所需满足处置需求的验证完成后结束。

运行使用验证和退役处置验证活动可能包括确认评估，即对系统达成所需的使命任务目的/目标程度的评估。

5.3.2.3 验证技术规程

验证技术规程提供步骤清晰的执行设定验证活动的指导。这个技术规程可能是试验、演示验证或任何其他验证相关的活动。使用的技术规程需要成文并提交到验证活动的试验准备状态进行评审和审批（参见 6.7.2.1 节中关于试验准备状态评审的论述）。

技术规程还用来验证设施、地面保障的电子/机械设备和特殊试验装置的验收。技术规程通常包含如下信息，当然可能根据不同的活动和受试产品而变化。

- 试验产品和材料的名称和标识；
- 试验技术状态辨识及其与飞行/运行技术状态的差异；
- 根据适当的验证规范为试验确定的目标与准则；
- 待检查与试验的特征和设计标准，包括接受或拒绝试验结果的阈值及容许偏差；
- 按顺序描述的执行步骤和需要进行的具体操作；
- 需要用到的计算机软件标识；
- 用于测量、试验和记录的装置标识、指定范围、精度和类型；

- 表明所需计算机试验程序/辅助设备和软件已在飞行/运行用硬件使用之前通过验证的证书；
- 针对可用的运行数据记录装备或其他自动试验装置的特殊说明；
- 显示试验装置、试验产品及测量点的标识、位置、内部关联的布局图、设计图和其他图表；
- 具有危险情形或操作的标识；
- 确保人员安全并防止试验产品和测量设备功能退化的安全防范说明；
- 需要在容许范围内维持的环境和/或其他条件；
- 检查或试验的约束；
- 关于需求不符或异常情况和结果发生时处理的特殊说明；
- 整个验证活动开始前到结束后，在设施和设备维护、内部管理、质量检查、安全性及处理需求方面的规范。

成文的技术规程在文本格式上留出空白以记录结果及叙述评论，从而形成完整技术规程并作为验证报告的一部分。所使用的经核准的技术规程副本作为项目的档案之一进行维护。

注：重要的是认识到在系统的寿命周期中，从费用或技术的角度看，需求可能变更或组件的退化可能导致设计方案过于困难而无法生产。在这种情况下，关键是在较低产品层次上应用系统工程设计流程确保改进设计提供合适的设计方案。应当评估决定所需变更的程度，并且流程应针对问题适当裁剪。可能需要修正合格性认证、验证和确认流程以确定新设计方案控制基线，并保持与前期描述的相关流程目的保持一致。验收试验也应根据需要更新，以验证新产品已经按照修正控制基线的设计进行制造或编码。

5.3.2.4 验证报告

应当针对每个分析，至少针对主要试验活动提供验证报告，这些活动如功能性试验、环境试验和全系统兼容性试验等，需长时间进行或与其他活动间隔。对于每个单独的试验活动，如功能性试验、声学试验、振动试验、热真空/热平衡试验，都需要验证报告。验证报告应该在试验后数周内完成，提供所针对的验证需求是否被满足的相关证据。

验证报告如下：

- 验证目标及达成目标的程度；
- 验证活动的描述；
- 试验技术状态及其与飞行/运行技术状态的差异；
- 每个试验与技术规程的特定结果，包括试验的注解；
- 每次分析的特定结果；
- 试验性能的数据表、曲线图、图解和照片；
- 关于正常结果的偏差、问题/失败、经核准的异常修正行动和重新试验活动的描述；
- 需求不符情况报告的概要，包括处理过程；
- 关于验证活动成功的结论和建议；
- 受试验影响的辅助设备的状态；
- 所使用技术规程的副本；
- 试验结果的鉴定及可接受性授权。

5.3.2.5 全系统试验

全系统试验的目的是演示验证接口的兼容性及系统内不同单元之间、分系统之间和系统整体预期应达到的所有功能。在集成地面及飞行系统上进行的全系统试验包括有效载荷的所有单元及其控制、启动、通信和数据处理，以演示验证整个系统能够以满足使命任务需求与目标的方式运行。

全系统试验包括在多个状态控制项上执行完整的线程或运行想定，以确保所有使命任务与性能需求得到验证。运行想定被广泛用于确保系统（或系统集成）能成功地实现使命任务需求。运行想定是关于系统如何运行、如何与用户及外部接口（如其他系统）交互的逐步描述。想定描述的形式应能方便工程师通读想定，理解系统的各个组成部分如何发挥功能和进行交互，以及验证系统满足用户的需求和期望。运行想定应能为所有确定的用户类型描述所有的运行模式、使命任务阶段（如安装、启动、正常与意外操作的典型实例、结束和维护），以及关键活动顺序。每一个想定都应该适当包含事件、行动、激励、信息、交互等，从而确保对系统的运行使用方面的综合理解。

图 5.3-3 给出一个科学卫星任务中的全系统数据流实例。图中每个箭头代表在两个硬件、软件、子系统、系统状态控制项之间的数据流和控制流。全系统试验验证遍及多系统环境中数据流的正确性、系统是否提供所需的功能性、最终的端点输出与预期结果的相应性。试验环境与真实的运行环境应尽可能近似，使得性能试验也包括其中。图中并没有显示全系统试验的全部范围。给出的每一个系统都需要分解到更小的粒度，保证试验的完整性。

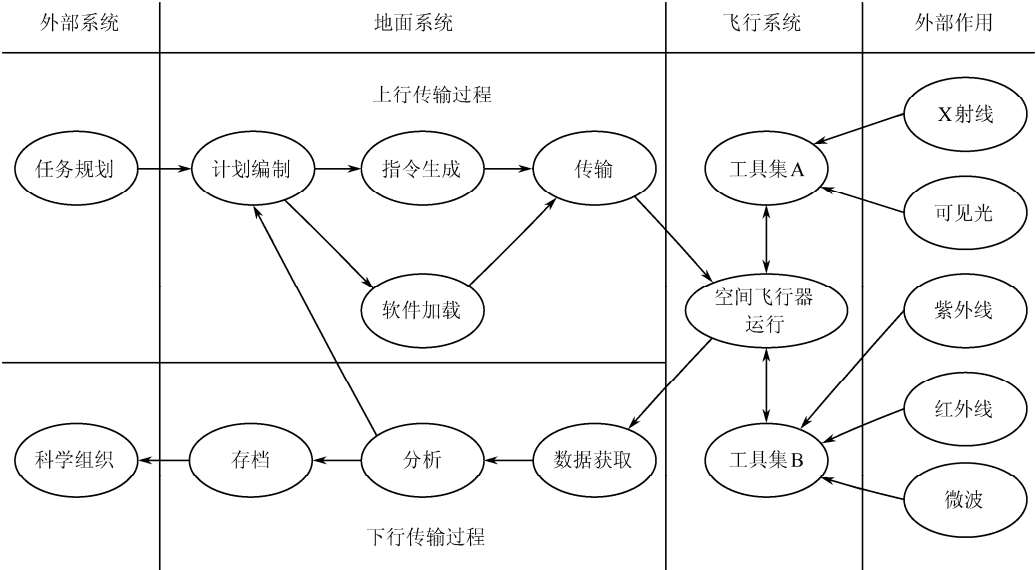


图 5.3-3 科学卫星任务中的全系统数据流实例

全系统试验是整个系统验证与确认的重要部分，也是在选定硬件、软件的系统寿命周期特定阶段应用的活动。与状态控制项试验相比，全系统试验仅考虑与其他系统的状态控制项（可能是硬件、软件或与人员有关的产品）进行外部交互层次上的状态控制项。状态控制项的内部接口（如软件的子程序调用、模/数转换接口）不在全系统试验的范围之内。

如何进行全系统试验

全系统试验可能是项目验证程序中最重要的一部分，试验应按照“以真实飞行方式试验”的原则进行设计。这就意味着，以实际技术状态组装系统，置放在真实的环境中，再以其所有的运行模式“飞行”。对无人科学使命任务，目标与外部干预应设计为向科学仪器提供真实输入。从科学仪器中输出的信号流向卫星数据处理系统，而后通过卫星通信系统传输到真实的地面站。如果数据通过一个或多个卫星或地面中继（如跟踪与数据中继卫星系统）传输到地面站，则所有中继必须包含在试验内。

全系统兼容性试验包括在所有使命任务模式下发生的完整运行操作链，以此方式确保系统满足使命任务需求。模拟的使命任务环境应尽可能地逼真，科学仪器应该接收到使命任务中所有类型的外部输入。无线电频率、地面站运行和软件功能全面进行试验。如果运行中系统的某些部分有可接受的仿真设施，可利用仿真设施替代真实系统单元进行试验。进行全系统试验，以及使用外部干预、有效载荷技术状态、无线电频率链路和其他系统单元的特定环境，必须根据使命任务的特征确定。

尽管全系统试验可能是系统验证程序中最复杂的试验，在各个系统层级上的试验仍需精心地准备。例如，必须指定试验负责人，选定试验团队并进行培训。必须留出充足时间进行试验计划及与设计团队协调。试验技术规程和试验用软件必须归档、审批，并置于技术状态控制下。

在进行系统所有组件之间的全系统试验之前，计划、协议、设施必须良好地准备就绪。

一旦试验开始，测试结果被记录，而任何偏差应仔细记录和报告。所有试验数据必须在技术状态控制下维护。

注：当使命任务是国际合作或与外部合作者共同开发时，这点尤为重要。

在完成全系统试验之前，需对每个状态控制项完成的活动如下：

- 每个状态控制项的所有需求、接口、状态及状态转移应通过综合试验技术规程和试验大纲进行试验以确保状态控制项的完整和正确。
- 对软件变量的完备集应当进行运行范围检查试验，以确保软件在其完整范围内如期使用，以及确保超出范围或条件时的适当错误警告。

全系统试验包括如下活动。

(1) 已经制定涵盖以下在任务执行过程中（常规、非常规和紧急条件下）可能发生的所有事项的运行想定。

- 任务阶段、模式和状态转移；
- 初次事件；
- 运行性能的下限与上限；
- 故障保护程序；
- 故障检测、定位和修复方法；
- 安全特性；
- 运行中对瞬时或非常规传感器信号的反应；
- 上行与下行通信。

(2) 在状态控制项开发的寿命周期内，用于尽早对状态控制项、接口和系统性能进行试

验的运行想定。这通常意味着应该尽快地制造模拟器或相应软件以实施运行全部想定。生成真实系统的模型与仿真/软件实现的或真实的状态控制项一起,尽可能早地运行全部想定是极端重要的。

(3) 所有接口的完整图形与详细目录已经归档。

(4) 执行试验大纲,涵盖人与人、人与硬件、人与软件、硬件与软件、软件与软件及子系统与子系统之间的交互,以及相应的输入、输出和运行模式(包括安全恢复模式)。

(5) 强烈建议在全系统试验中,选择以前没有参加过试验的操作人员按照系统预定的使用方式操作系统,已确定系统是否会失败。

(6) 试验环境应尽可能与真实运行环境相似/相仿。试验环境的逼真度应经过有效性鉴定。试验环境与真实运行环境之间的差异应在试验或验证计划中归档。

(7) 如果需求无法试验,验证可以通过其他手段(如模型校验、分析或仿真)进行。如果真实的全系统试验无法实施,试验必须通过分析和仿真分片进行,并拼接在一起。此类实例如在轨集成的系统,其中各类单元的首次拼接在轨完成。

(8) 如果识别并定位已开发系统存在的缺陷,需对系统或组件进行回归试验,以确保系统修正没有带来意想不到的影响,系统或组件满足先前试验过的特定需求。

(9) 如果试验失败或试验存在缺陷(如由技术状态或试验环境引起),应在问题定位后重新进行试验。

(10) 运行想定应该应用在制定运行使用计划中。

(11) 系统交付之前,作为系统合格性试验的一部分,试验大纲应当以使命任务中可能发生的顺序遍历在运行使用计划中安排的所有计划。

全系统试验归档应包括如下内容:

- 以全系统试验计划为一部分的验证或试验计划。
- 技术状态控制下的文档、表格或数据库,用于试验方案和结果。其中,数据包括试验大纲标识、试验的子系统/硬件/程序集合、验证的需求清单、试验的接口、试验日期和试验结果(即试验的真实输出与预期输出的一致性)。
- 全系统试验大纲与技术规程(包括输入与期望输出)。
- 全系统试验中的问题/失败/异常记录。

全系统试验可以与其他项目试验活动集成,但是本节所提到的文档应当可以随时被抽取出来对其状况进行评审、评估。

5.3.2.6 建模与仿真

对于产品验证流程,模型是待验证目标产品的物理的、数学的或逻辑的描述。不管是在寿命周期早期或后期,建模与仿真都可以用来增强支持产品验证流程,是进行产品验证的有效工具。仿真工具和模型自身皆使用系统设计和产品实现流程进行开发。

应用的模型及仿真工具作为辅助产品,在其开发与实现(包括使用团体的验收)中必须应用 17 个技术流程(见 NPR 7123.1《NASA 系统工程流程和需求》),以确保建模与仿真适当表现出运行使用环境及目标产品模型的性能。此外,某些情况下,建模与仿真应用的合理性应在实际应用前得到证明。

建模与仿真资源有很多的来源,例如,来自能够提供阐述特定系统属性模型的承包商、政府机构或实验室。

注：物理模型、数学模型、逻辑模型的开发包括对模型的评估，评价模型是否根据产品设计方案提出的模型需求进行开发，能够代表所实现的系统目标产品，评价其作为模型是否有效。在某些情况下，模型必须经过认定，证明其可应用于特定范围。就像其他辅助产品一样，对验证系统目标产品可用性的模型，其生成和评价也要有预算和时间的计划。

5.3.2.7 硬件在回路

功能完全的目标产品，如实际的硬件，可以与模拟其他系统目标产品输入/输出的模型和仿真结合，这称为“硬件在回路”试验。硬件在回路试验在综合环境中将所有系统单元（子系统或试验设备）连在一起，提供对真实系统或子系统的高逼真度实时的运行评估。操作人员可能与试验紧密相关，而硬件在回路资源也可以在分布试验和分析应用中与其他设备连接。硬件在回路试验的应用价值之一在于尽可能与真实的系统接近，当运行环境难于再现或费用昂贵时，可以支持验证与确认工作。

在开发阶段，这种硬件在回路验证通常发生在总体实验室或相关试验设施。例如，硬件在回路可以是特定实验室中完整的空间飞行器，其输入/输出来自于模拟实际运行环境中的系统模型。实时计算机用于控制项目运行想定中的空间飞行器及子系统。根据制导和控制系统硬件/软件发出的指令，实时进行飞行动力学模拟，以确定飞行轨迹并计算系统飞行状态。硬件在回路试验可用于验证被评估的目标产品是否满足接口需求，是否适当地将输入转化为所需要的输出。硬件在回路可以通过模拟目标产品的输入或输出而评估输出的质量，为在系统结构中较低层级的实物目标产品试验提供有价值方法。这种方法可以在工程或项目的全寿命周期使用。航天飞机工程中应用硬件在回路来验证其主发动机的控制软件与硬件。

建模、仿真、硬件/人在回路技术，若恰当地集成在试验中并有序进行，可以提供费用合理的验证方法。特别是这种集成试验流程有如下优点：（1）减少寿命周期试验费用；（2）发现所评估系统更有价值的工程技术/性能；（3）减少试验时间并降低项目风险。该流程还极大地减少产品寿命周期中破坏性试验的数量。验证试验中集成建模仿真技术可以洞察系统或子系统性能的变化趋势，而这在硬件的局限性约束下可能做不到。

5.4 产品确认

产品确认流程是对已实现目标产品验证与确认流程的第二个流程。验证证明“系统被正确实现”，而确认证明“实现的是正确系统”。换言之，验证为每个“需要”陈述是否被满足提供客观证据，而确认则针对客户与用户的利益进行，确保系统在设定的环境中以预期的方式完成其功能。这一点需要通过检查系统结构中每个层次上的产品而达到。

确认证实已实现的系统结构中任何层次目标产品满足其在运行使用构想中规定的利益相关者期望，并确保确认中发现的任何异常已在产品交付之前恰当地解决。本节论述该流程活动，包括其类型、输入和输出，以及潜在的缺陷。

产品验证与产品确认的辨异

从流程的角度看，产品验证与产品确认在性质上可能相似，但是它们的目标却根本不同。

从客户的观点看，其关注点是所得到的目标产品是否在使用环境中按照预期工作。证实

已实现产品与相应的产品规范和设计描述文档一致是必要的，因为这些规范和文档建立产品的技术状态控制基线，而这类控制基线在以后可能必须修改。如果没有经过验证的控制基线与合适的技术状态控制，后期的修改可能导致成本增加或产生性能问题。

若经过分析能证实其有效且有保证，可应用各种组合试验。在进行确认之前，确保系统结构中每个产品是按照特定需求实现的，将减少确认试验的开支。

验证测试与确认测试辨异

- **验证试验**：验证试验与批准的需求集合（如系统需求文档）相关，在产品寿命周期的不同阶段执行。

验证试验如下：

- 用于辅助产品、产品单元的开发与定型及辅助制造或保障流程的试验；
- 用于验证技术成熟状态，验证技术风险已最小化，证实合同技术性能已实现，以及证明初步确认试验准备工作已就绪的工程技术类型的试验。验证试验使用测量设备和度量指标，通常由工程师、技术人员、操作维护人员等试验者在有利于失效分析的受控环境中完成。
- **确认试验**：确认试验与运行使用构想文档相关。确认试验针对任何目标产品在真实环境或模拟环境中进行，目的是确认由典型用户使用的产品在执行使命任务时的有效性与适用性；并对试验结果进行评估分析。试验是适用于验证与确认的详细的定量方法。当然，试验需要确认待生产和部署的目标产品的有效性。

5.4.1 流程描述

图 5.4-1 给出了产品确认流程的典型流程图，并确定产品确认所应考虑的典型输入、活动及输出。

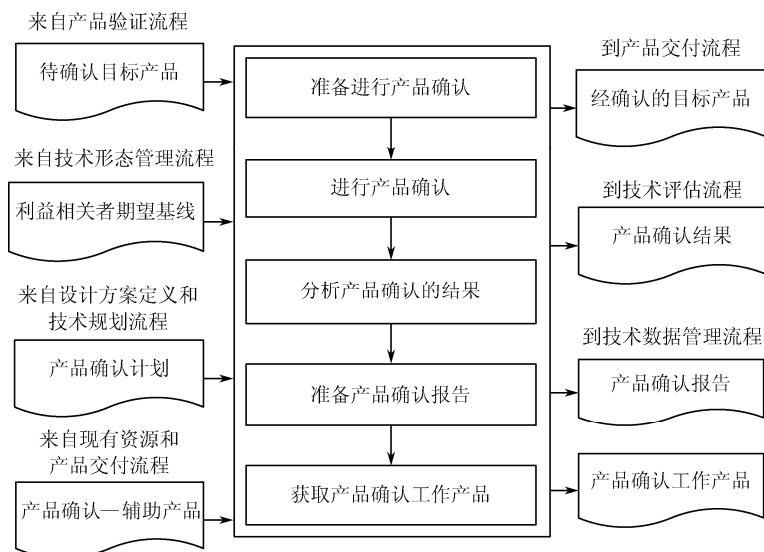


图 5.4-1 产品确认流程

5.4.1.1 输入

确认流程的关键输入如下：

- 经过验证的产品；
- 确认计划；
- 已确定控制基线的利益相关者期望（包括运行使用构想和使命任务需求与目标）；
- 执行产品确认流程所需的辅助产品。

5.4.1.2 流程活动

产品确认流程用于演示验证已实现的目标产品在预定的运行环境下，由预期的操作人员或用户使用时，能够满足利益相关者（客户或其他关注团体）的期望。确认的类型决定于寿命周期阶段和产品在系统结构中所处的位置。

确认流程有如下 5 个主要步骤：（1）确认计划（准备实施确认的计划）；（2）确认准备（准备执行确认）；（3）执行确认（按计划进行确认）；（4）分析确认结果；（5）获取确认工作产品。

产品确认流程的目标如下所述。

- 证实下述各项。
 - 已实现正确的产品——客户想要的。
 - 已实现产品可以被操作人员或者用户使用。
 - 产品满足效能度量指标。
- 证实已实现产品在预定的环境中使用时满足预期的使用要求。
 - 从系统结构（最终 WBS 模型）自底层向上直到顶层产品，对每个已实现（制造或集成）的产品进行确认。
 - 证实产品结构每一层的产品满足能力需求或满足客户/用户/操作人员和其他关注团体多方面期望的证据已经获取。
- 确保发现的问题在已实现产品交付之前（如果确认由产品供应商完成）或在产品与其他产品集成为更高层产品之前（如果确认由产品接收者完成）被有效地解决。

验证与确认分别描述为两个流程，但实际使用时有很多的重叠。若经分析证实费效比高且有保证，可应用各种组合试验。然而从流程角度看，验证与确认在性质上相似，目标却根本不同。

从客户的观点看，关注点在于所得到的目标产品在设定的使用环境中能否提供所需的能力。在确认之前，在验证中确保系统结构中每个目标产品按照其特定需求正确实现将会减少单独进行确认试验的开支。有可能系统设计没有适当完成，这样尽管验证试验是成功的（满足特定需求），但是确认试验仍将失败（不满足利益相关者期望）。所以，对系统结构中的低层产品进行验证及确认是非常必要的，这样可以尽早的发现产品设计中的失效和缺陷。

1. 产品确认计划

进行产品确认计划编制是关键的第一步。使用何种确认类型（如分析、演示验证、检查、试验）需要考虑以下因素：已实现产品的形式，产品所处的寿命周期阶段、成本、进度、可用资源，产品在系统结构中所处位置（产品验证与确认计划概要的实例参见附录 I）。

应当建立待确认的需求集合或子集，而对确认计划（基于设计方案在技术规划流程中的输出）的评审应当针对特定的技术规程、约束、成功准则或其他确认需求。应当建立产品进行确认时的条件 and 环境，并依据相关寿命周期阶段和确定的成功准则制定确认计划。需要应用决策分析流程辅助编制最终计划中的一些细节。

与利益相关者共同评审确认计划，并理解产品确认时与实际使用（有人参与）时所处背景之间的关联是非常重要的。作为计划流程的一部分，应确定进行确认的辅助产品，并开始进度安排和采办。

应根据计划的确认类型（如分析、演示验证、检查、试验）准备进行确认的技术规程。这些技术规程通常是在项目寿命周期的设计阶段开发并伴随设计不断成熟。需要思考运行和使用案例想定，以便开发所有可能需执行的确认活动。

确认的类型

- **分析：**基于计算数据或来自系统结构较低层次目标产品确认的数据，应用数学建模与分析技术预测产品设计对利益相关者期望的适合性。通常在产品原型、工程模型或制作/组装/集成的产品不可用时使用。分析包括建模与仿真的应用。
- **演示验证：**直接使用目标产品显示利益相关者期望能否达到。它通常作为证实性能指标的基础，同时不需要收集详细数据，显示出与试验的区别。对系统结构中所有目标产品在真实环境中进行确认，目的是确定在用于 NASA 使命任务或典型用户使命任务中产品的有效性与适用性，并评价试验结果。
- **检查：**对已实现目标产品的表现检查。通常用来确认产品的物理设计特性或辨识特定制造商。
- **试验：**使用已实现目标产品获取详细数据以确认产品性能，或通过进一步分析为确认性能提供足够信息。试验是验证与确认的详细定量方法，但它也是确认待生产和部署的目标产品所必须的。

2. 确认计划和方法

确认计划是技术规划流程的工作产品之一，生成于产品设计方案流程，以根据设定的控制基线确认所实现产品是否满足利益相关者期望。确认计划有多种形式。确认计划描述在系统结构中从底层到顶层的目标产品开发的试验与评价计划，并贯穿从试验与评价到生产，再到验收的各阶段。确认计划同时包括验证与确认计划（验证与确认计划概要实例参见附录 I）。

确认的类型包括试验、演示验证、检查和分析。尽管每个方法的名称与验证计划中方法名称一样，但是目的和意图是不同的。

确认由用户/操作人员或由开发者完成，具体由 NASA 中心指令或与开发者签订的合同确定。系统级确认（如客户试验与评价和其他确认类型）可以由采办方试验团队进行。对由开发者进行确认的部分，必须达成适当协议，确保确认证明文档与已实现产品共同交付。

所有已实现的目标产品，不论来源（购买、制造、重用、组装或集成）及在系统结构中的位置，必须确认以证实其满足利益相关者期望。确认中发现偏差、异常、需求不符等情况，应当与解决这些差异的行动一起归档。确认通常发生在模拟或真实运行条件下设定的运行使用环境中，而不像产品验证流程那样在受控条件下进行。

针对各种各样的产品形式，确认可以在项目全寿命周期中递归执行，产品形式如下：

- 模拟件（算法模型、虚拟现实仿真器）；
- 样机（木质样品、硬试样、软试样）；
- 概念描述（纸质报告）；
- 原型（具备部分功能的产品）；
- 工程元件（具备所有的功能，但形式可能不同）；
- 设计确认试验元件（形式、尺寸和功能相同，但可能没有飞行部件）；

- 合格元件（与飞行元件一致，但承受极端环境）；
- 飞行元件（飞行的目标产品）。

以上类型产品形式可能处的状态如下：

- 生产（构建、制作、制造、编码）；
- 重用（修改内部开发的产品、修改购买的现货产品）；
- 组装或集成的产品（低层次产品的组合）。

注：对目标产品的官方正式确认应当针对可控产品进行。通常，试图根据使用构想在原型上进行最终确认不可接受，通常应在经过合格验证的、最终飞行的可控单元上进行。

确认计划所产生的成果包括如下所述。

- 适合证实已实现产品满足利益相关者期望的确认类型（基于已实现产品的形式）已经确定。
- 确认技术规程完成制定如下：
 - 选定的确认类型所需要的技术规程；
 - 技术规程步骤的目标与目的；
 - 试验前与试验后的活动；
 - 确定技术规程成功或失败的准则。
- 确认技术规程所需的确认环境（如设施、设备、工具、仿真、测量装置、人员和运行条件）已经定义。

注：在制定确认计划时，应该考虑完成确认试验的范围。在许多实例中，要综合利用非常规运行想定与常规运行想定。通过非常规试验，可以加强对整体性能特征的把握，并且可以辅助辨识设计中的问题，确定人机接口、训练和技术规程变更，以满足任务目的和目标。在制定确认计划时，非常规试验与常规试验都应该包括在内。

3. 产品确认准备

为准备执行产品确认，应获取建立确认计划所依据的相应期望集合。同样，为进行确认应当获取待确认的产品（来自产品实施执行或集成/验证流程的输出），以及确认所需的辅助产品与保障资源（设计方案启动的需求辨识和采办活动）。

确认准备所需的辅助产品和保障资源示例

在产品确认流程中，“进行确认准备”的关键任务之一是获取进行确认所需的必要的辅助产品与保障资源。该任务需获取的产品和资源实例如下：

- 度量工具（度量范围、电子装置、探测器）；
- 嵌入式试验软件；
- 试验布线、测量工具及遥感装备；
- 记录装置（获取试验结果）；
- 硬件在回路仿真中的目标产品（软件、电子器件或机械部件）；
- 其他系统的外部接口产品；
- 其他系统的现实外部接口产品（飞行器、车辆、人类）；
- 灵巧熟练的操作员。

完成确认环境准备（确认中涉及到的安装设备、传感器、记录装置等）和确认技术规程评审，确定和解决影响确认的问题。

确认准备的成果如下：

- 完成执行确认计划的准备工作；
- 已获取可用的利益相关者期望集；
- 用于确认的物品和模型及待确认的产品和辅助产品已按照计划与进度集成在确认环境中；
- 按照计划与进度，已获取可用资源；
- 已对确认环境的适应性、完备性、准备状态和集成性进行评估。

4. 按计划进行产品确认

目标产品的确认工作将按照在确认计划与技术规程中阐明的那样进行，并与每个特定的确认需求一致。责任工程师应当确保技术规程按照计划被遵从和执行，确认所需辅助产品被正确校验，确认针对需确认指标的数据被收集和记录。

如果确认的设计和实施执行是低劣的，或确认条件引起异常情况，此时应该根据需要重新做出确认计划，纠正产生异常的环境准备，并根据改进或更正的技术规程和资源重新进行确认。针对识别的问题应当使用决策分析流程，这些决策内容可能包括需要评价备选方案并做出选择，或需要对确认计划、环境和/或实施执行做出变更。

进行确认所得到的成果如下：

- 经确认的产品，同时建立支撑证据，表明相应结果已经收集并评估，说明确认目标已完成。
- 对制作/制造、组装或集成的产品（包括可用的软件和硬件产品）是否满足相应利益相关者期望所做出的判断。
- 关于被确认产品是否与确认环境恰当集成及选定的利益相关者期望是否被适当确认所做出的判断。
- 关于待确认产品是否与关联产品共同在其性能允许范围内正常工作所做出的判断。

5. 分析产品确认结果

确认活动一旦完成，即收集结果并分析数据来证实所提供的目标产品在既定的应用环境中满足客户需要的能力，证实确认技术规程被遵守，并且辅助产品和保障资源正确工作。这些数据还用来分析质量、完整性、正确性、一致性和有效性，任何不合适的产品或者是产品属性应该被辨识并报告。

将实际确认结果与期望结果进行对比，重新进行所需的系统设计与产品实现流程活动以解决产品缺陷是非常重要的。需要时，产品缺陷，以及建议的更正行动和解决方案应当归档，并重复确认流程。

分析确认结果所得到的成果如下：

- 产品的缺陷和/或识别的问题。
- 关于解决异常、偏差和需求不符合条件（进行非低劣确认时出现的问题）已得到相应的重新计划、需求定义、设计和重新确认的保证。
- 需要时，偏差及更正行动报告已经生成。
- 完成的确认报告。

6. 确认的注意事项

使用的确认类型依赖于寿命周期阶段、产品在系统结构中的位置、可用的费用、进度和资源。在同一系统模型内的产品确认可以共同进行（如目标产品及其相关辅助产品，可以是运行情况下的控制中心或雷达及相关显示器，维修情况下的产品及维修工具，或后勤保障时的运载火箭或运输机）。

系统结构中每一个已实现的产品在向高层产品集成之前，应根据利益相关者期望进行确认。

7. 流程重组

基于产品确认流程的结果，需要对有缺陷的目标产品进行流程重组。改正单个或多个缺陷时应当小心，不能使前期运行令人满意的部件或性能产生新的问题。回归试验作为一种主要用于软件的正式流程，在重新运行前期验收试验流程时，能够确保变更不影响前期验收功能和性能的方法。

注：必须注意的是，要确保已明确的用于移除确认缺陷的纠正行动，在该项变更未与相应利益相关者协调情况下，不会与已确定控制基线的利益相关者期望相冲突。

8. 确认中发现的缺陷

确认结果若不能令人满意可能有若干原因。一个原因是确认流程执行不力（例如，辅助产品和保障资源缺失或功能不正确，操作员未经训练，未按照技术规程执行，设备没有校准或确认环境条件不合适），且未能控制没有列入确认利益相关者期望集的其他有影响的变量。另一个原因可能是目标产品的验证流程中出现缺失。如此产生以下需求：

- 重组系统结构中产生有缺陷（未能满足确认需求）产品的低层目标产品；
- 重新执行必要的验证与确认流程。

确认流程发现缺陷的其他原因（特别是在建模与仿真中）可能有不正确或不合适的初始条件或边界条件，方程或行为模型不完善，方程或行为建模中近似处理的影响，没有为可靠的特定仿真提供几何上/物理上所需的逼真度，以不完善或未知的不确定性量化水准作为参考依据，建模仿真中物理现象在空间上、时间上和统计上可能存在分辨率缺陷。

9. 获取产品确认流程的工作产品

确认的工作产品（输入到技术数据管理流程）具有多种形式，包含多个信息源。获取并记录与确认相关的数据是产品确认流程的重要步骤，但却常常被忽视。

应当获取确认结果、所发现的缺陷及更正行动，还有来自产品确认流程应用的相关结果（如相关决策、决策的依据、假设和经验总结）。

获得确认工作产品的成果如下所述。

- 进行产品确认流程活动的工作产品和相关信息，以及记录的任务，即确认类型、用于确认的目标产品形式、确认技术规程、确认环境、结果、决策、假设、纠正行动、经验总结等（通常用矩阵或其他工具完成——参见附录 E）。
- 辨识和归档的缺陷（如偏差、异常、需求不符的情况），包括解决问题采取的行动。

- 为已实现产品与确认中使用的利益相关者期望集相一致提供的证据。
- 确认报告如下：
 - 确认结果/数据记录；
 - 所用利益相关者期望集的版本；
 - 确认用目标产品的版本与形式；
 - 所用工具或设备的版本和标准，以及可用校准数据；
 - 包含在成功/失败声明中的每个确认的结果；
 - 实际结果与期望结果之间的差异。

注：对于只需开发单个交付产品的系统，产品确认流程通常同时完成验收试验。然而应当了解，对于同一产品部件需要多个系统，按照第一个交付件那样对后续部件进行验证与确认并不是可取的方法。相应地，验收试验是确保后续交付件符合设计控制基线的更合适的方法。

5.4.1.3 输出

确认的关键输出如下：

- 确认的产品；
- 缺陷报告及相应的纠正行动；
- 确认报告。

该流程的成功准则如下：

- 产品性能的客观证据和每个所关注系统的确认活动结果已归档；
- 在所有解决问题行动结束之前不能认为和认定确认流程已经完成。

5.4.2 产品确认指南

以下是产品确认流程的一般性指南。

5.4.2.1 建模与仿真

如验证流程中所强调的，建模与仿真是重要的确认工具。考虑使用建模与仿真时涉及到建模与仿真自身的验证、确认和认定。

模型的验证与确认

- **模型验证：**模型精确满足其规范的程度，回答“这是想要的吗”问题。
- **模型确认：**从模型应用的角度，确定模型精确表达现实世界程度的流程。
- **模型认定：**针对特定目的鉴定模型的应用。回答“是否应该认可模型”问题。

5.4.2.2 软件

软件验证是一项软件工程活动，演示验证软件产品满足特定需求。软件验证的方法有发现软件工程产品的缺陷所进行的同行评审/检查、应用仿真方法对软件进行需求验证、黑箱与白箱试验技术、需求实施情况分析、软件产品演示验证。

软件确认是一项软件工程活动，演示验证建成的软件产品或软件产品组件在预定环境中发挥预期效用。软件确认的方法有仿真环境中软件产品组件行为的同行评审/检查，依据数学模型、分析、运行使用环境演示验证的验收试验。项目中软件验证与确认的方法应在软件开发计划中明确。特定的 NASA 总局级层软件验证与确认需求、同行评审需求（参见附录 N）、试验和报告需求包含在 NPR 7150.2 《NASA 软件需求》中。

用于软件验证与确认的严苛条件与技术取决于软件的分类（与项目及有效载荷的分类不同）。复杂项目通常包括若干拥有不同软件分类的系统与子系统。对于项目而言，重要的是进行软件分类，计划验证与确认方法，适当考虑各个分类相应的风险。

例如，NASA 的管理层可能选择由西弗吉尼亚州费尔芒特的 NASA 软件独立验证与确认机构对项目进行额外的独立的软件验证与确认。在这种情况下，需要制定谅解备忘录并执行每个软件的独立验证与确认计划。

5.5 产品交付

产品交付流程是用于将产品实施执行或产品集成所得的目标产品，经验证与确认后交付到系统结构较高层次的客户，以集成该层目标产品或将顶层目标产品交付给既定的最终用户。产品交付的形式主要依赖于相关产品寿命周期阶段的成功准则，以及目标产品相应的工作分解结构模型在系统层次结构中的位置。

产品交付可能发生在寿命周期的所有阶段。在早期阶段，技术团队的产品是文档、模型、研究报告。随着项目寿命周期的推进，这些纸质产品或软产品通过实施与集成流程转换为硬件产品与软件产品，以满足利益相关者的期望。产品交付流程在寿命周期中以不同的严格程度重复，包括产品在系统结构中向更高层次交付。产品交付流程是产品实现流程中的最后一个流程，是低层次系统通向更高层级的桥梁。

产品交付流程是将活动、子系统或单元连接到整个工程系统的关键。随着系统开发接近完成，产品交付流程再次应用于目标产品，但由于交付目标是将最终的系统级产品交付给实际的用户，因而交付条件更加严格。根据所开发系统的种类，交付工作可能涉及 NASA 中心或总局，并牵涉到数千人，需完成多个目标产品的存储、处理和运输，准备交付场所，培训操作人员与维护人员，安装与维护系统。例如，将外部推进剂箱、固体火箭助推器和轨道器交付肯尼迪航天中心完成集成与发射。

5.5.1 流程描述

图 5.5-1 呈现了产品交付流程的典型流程图，确定产品交付流程中需要考虑的典型输入、活动和输出。

5.5.1.1 输入

产品交付流程的输入主要依赖于交付的需求、待交付的产品、产品交付采取的形式、产品交付的对象和地点。典型的输入如图 5.5-1 所示，详细讨论如下所述。

(1) 待交付的（多个）目标产品（来自产品确认流程）。

待交付产品可以有多种形式，可以是子系统组件、组装的系统或顶层目标产品，可以是

硬件或软件，可以是新开发、购买或重用的产品。产品可以通过与其他交付产品集成，从系统低层交付到高层产品。交付流程可能重复，直到得到最终系统产品。在准备交付已确认的产品到更高层次时，交付流程需要考虑输入的一致性。

早期阶段产品通常应用解析或物理模型进行基础或应用研究，得到纸质或电子文档形式的信息或数据。实际上，许多 NASA 研究项目或科学活动的目标产品是报告、文档甚至口头汇报。某种意义上，NASA 研究与开发所得信息的传播是产品交付的重要形式。

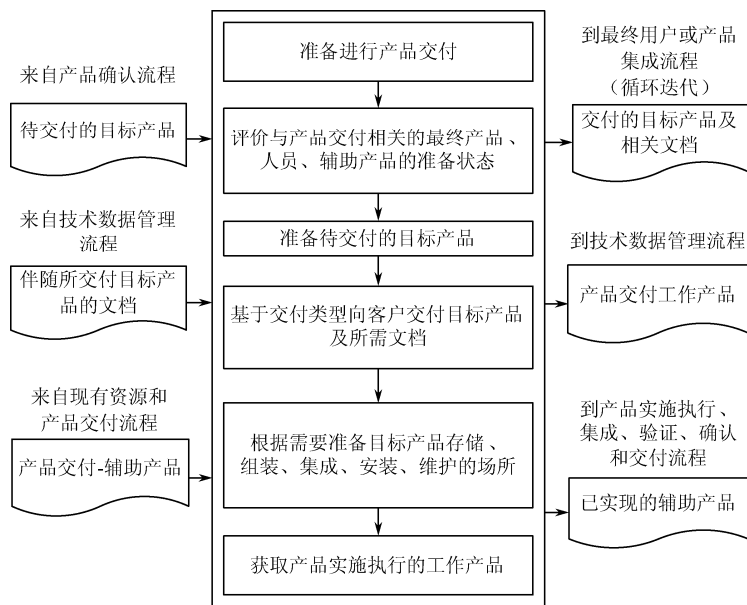


图 5.5-1 产品交付流程

(2) 目标产品附属文档，包括手册、技术规程和流程说明（来自于技术数据管理流程）。

产品交付流程所需文档决定于特定的目标产品、其在系统结构中当前所处的位置、在各种协议/计划/需求文档中确定的需求。通常产品有唯一标识（即序列号），可能还有一个“家谱”（档案），指定其来源和当前的状态。有关的信息可以通过技术状态管理系统、工作指令系统，以及设计图或试验报告归档。文档中通常包括验证与确认一致性的证明。现货产品通常包含制造商提供的规格书或说明书。文档还可能包括操作手册、安装指南或其他有用信息。

文档的详细程度将依赖于产品在系统结构中的层次与产品所处的寿命周期阶段。在寿命周期的早期，文档可能只是初步性质说明。在后期阶段，文档可能是详细设计、用户手册、设计图纸或其他工作产品。交付阶段输入过程所获得的文档可能需要编辑、组装或重新包装以确保达到客户可接受的条件。

必须专门考虑安全性，包括用清晰的标签或标记来识别危险材料的使用、特殊操作的指导和存储需求。

(3) 交付的辅助产品，包括包装材料、容器、操作设备，以及存储、接收、运输设施（来自辅助产品实现的已有资源或产品交付流程）。

产品交付的辅助产品可能有利于向较高层次交付产品的实施、集成、评价、交付、训练、操作、保障及退役，或有利于最终系统产品的交付。部分或全部的辅助产品可在与交付相关的协议、系统需求文档或项目计划中定义。某些情况下，产品交付的辅助产品在产品自身实现时开发或可能需要在交付阶段开发。

随着产品的开发，特殊容器、支架或其他设备也需要同时开发以在产品开发和实现过程中辅助产品的存储与运输。这些设备可能是临时使用，也许不能满足交付的所有需求，但又是产品进入交付阶段必不可少的。在这种情况下，临时设备必须改进或重新设计制造，或采购新的临时设备，以满足特定的运输、处理、存储和转运需求。

敏感或危险的产品可能需要特别的辅助产品，例如，监控设备、检查装置、安控设备或人员培训以确保达到并维持充分的安全性和环境需求。

5.5.1.2 流程活动

产品的交付可以采取以下两种形式之一：

- 低层系统目标产品交付到较高层次并集成成为另一个目标产品。
- 最终系统产品交付给客户或用户，在真实环境中运行使用。

在第一种情况中，目标产品是集成在一起的若干产品之一，以形成第二种情况中交付给用户使用的产品。例如，目标产品可能是若干电路板之一，集成起来得到最终交付的产品。而集成的产品也可能是若干单元之一，必须再集成以形成最终产品。

交付的产品形式不仅依赖于产品在系统层次结构中的位置，还依赖于产品所处的寿命周期阶段。在寿命周期早期阶段，产品的形式可能是纸质或电子文件、物理模型、技术演示验证原型。后期阶段，产品可能是生产样机（工程模型）、最终研究报告或飞行器件。

图 5.5-1 给出在不考虑产品层次与寿命周期阶段情况下，产品交付过程的输入、输出及活动类型。这些活动包括准备进行交付，确保交付的目标产品及所有人员、所有辅助产品已准备就绪，准备交付场所，执行产品交付并获取和归档所有工作产品。

活动如何进行及文档应采取何种形式，同样依赖于产品在系统层次结构中的位置与产品所处寿命周期阶段。

1. 准备实施产品交付

第一项任务是确定产品交付采取如下哪一种形式：（1）低层目标产品交付到较高层级并集成成为其他目标产品；（2）最终系统产品交付给客户或用户，在真实环境中运行使用。交付的产品形式将直接影响交付计划及所需的包装、处理、存储和运输的类型。客户与其他利益相关者的期望，连同特定的设计解决方案，共同决定产品特定交付技术规程或包装、存储、处理、运输、站点准备、安装、保障所需要的辅助产品。这些需求应该在准备阶段进行相应的评审。

产品交付准备的其他任务包括确保目标产品、人员、所有辅助产品已经为交付准备就绪。这包括与目标产品共同交付的文档可用性证明，以及验证与确认一致性的证明。文档的适当详细程度依赖于产品在系统层次结构中所处位置与产品所处寿命周期阶段。在寿命周期早期阶段，这些文档可能是初步的性质描述。在寿命周期后期，文档可能是详细设计文档、用户手册、设计图纸或其他工作产品。执行交付的必要技术规程应当评审并通过审批。这包括系统工程管理计划中规定的在管理、法律、安全、质量、所有权等方面必要的审批。

最终，产品交付所需要的人员能力与技能，以及必要的包装材料/容器、处理设备、存储设施、运输设备的可用性应进行评审。任何为完成任务而对人员进行的特殊培训也应该在此阶段完成。

2. 准备交付的产品

当产品交付到较高层次进行集成或组装时，或将产品跨越国土运送给客户使用时，应当

格外小心注意确保产品运输的安全性。包装、处理、存储及运输的需求应在系统设计阶段确定。当产品需要存储或需要在不同的组织及其设施之间通过陆路、空中或海上交通工具运输时，为产品准备相应的包装以保障产品的安全并防止变质是一项非常重要的工作。需要特别关注的是，表面保护使其免受物理损伤、防止化学腐蚀、消除对电线电缆的破坏、震荡挤压损坏、受热变形和受冷破裂、受潮或其他颗粒侵入损坏相关部件。

在设计需求中应考虑产品处理与运输的方便性，如组件支撑、附加的运输挂钩、板条箱等。产品包装和拆包的安全性及简便性也应在设计中考虑。可能需要实施附加的度量指标以保证产品状态记录在案，或在运输过程中安全追踪产品。如果任务牵涉到危险材料，应制定特殊的标识和处理措施，包括运输线路。

3. 准备接收产品的场站

对任何一种类型的产品交付，都要准备好产品接收场站。在此场站中，根据产品在系统结构中的位置和寿命周期阶段、客户协议，对产品进行存储、组装、集成、安装、使用和维护。

大量关键性复杂活动，尽管不是技术团队直接控制，必须同步以确保产品向用户的平稳交付。如果交付活动未能细致控制，可能影响目标产品的进度、成本、安全性。

为了明确问题和需求，需要进行场站调查。应当考虑现有设备对新的目标产品验收、存储和操作的适用性，识别必要而未计划的后勤保障辅助产品和服务。此外，对现有设备的任何更新必须在实施之前周密计划，因此，场站调查应在产品寿命周期的早期阶段开展。可能包括后勤保障辅助产品和服务，为目标产品的运行、维护、退役提供保障。可能需要进行用户、操作人员、维护人员和其他保障人员的培训。在接收目标产品之前，需要依据国家环境保护法令得到相应批准。

运送前和接收后，目标产品可能需要存储在合适的存储条件下，以保护产品不受损伤或是侵蚀。这些条件应在寿命周期的早期阶段确定。

4. 交付产品

随后，基于选定的交付类型将目标产品及相关文档交付（即移交、运输、转送）到客户，例如，交付到工作分解结构较高层进行产品集成，或直接交付用户。交付的文档可能包括操作手册、安装指南和其他信息。

按照预先批准的安装技术规程，目标产品在较高层次中组装，或是在客户/用户的站点安装。

5. 确定保障准备就绪

不论是在较高层组装，或是安装到最终客户场站，此后应当进行交付后产品的功能试验与验收试验。这确保在运送/安装过程中产品没有受到损伤，可开展工作并准备实施保障。对最终交付的工作产品应当获取产品验收文档。

5.5.1.3 输出

(1) 向系统结构更高层次集成交付的目标产品：这其中包括相应的文档。产品形式及可用文档与产品在系统层次结构中所处位置及产品所处寿命周期阶段有关（目标产品的形式可能是硬件、软件、模型、原型、试验用初样、一次性产品或批量生产产品）。文档包括安装、

操作、使用、维护和培训的概要手册，可用的控制基线（技术状态控制基线、规范、利益相关者期望）文档，以及反映目标产品验证与确认已完成的试验结果。

（2）向最终用户交付使用的最终产品：需交付的目标产品及其相应文档应经过适当包装作为可运行使用的最终产品交付。文档包括产品最终的安装指南、操作手册、用户手册、维护手册、培训手册、控制基线（技术状态控制基线、规范、利益相关者期望）文档，以及反映最终产品验证与确认已完成的试验结果。如果由最终用户进行最终产品确认，应与最终产品同时交付能支撑最终用户确认活动的充足文档。

（3）交付活动中需提交到技术数据管理的工作产品：包括交付计划、场站调查、度量指标、训练模块、技术规程、决策、经验总结、纠正行动等。

（4）交付相应寿命周期保障组织的已实现的辅助产品：在各个阶段开发的某些辅助产品包括制造与集成用专门机械、工具、夹具，制造流程和手册，集成流程和手册，专用的检查、分析、论证、试验设备、工具、试验台，专门的包装材料与容器，处理设备，存储站点的环境，运输/传送的车辆或设备，专门的培训课件，工作场站的环境，交付的培训手册。在寿命周期的后期阶段，需要交付的辅助产品还包括专门的任务控制设备，数据采集设备，数据分析设备，操作手册，专用维护设备、工具、手册和备件，专用修复设备，退役处置装置，维修与退役处置必备的站点环境。

如下活动完成以后，交付流程即完成。

- 除非确认工作已在集成之前由集成人员完成，必须对照利益相关者期望完成目标产品的确认工作。
- 对于交付到集成的情况，目标产品应交付到条件适合的预定场站，以便与其他目标产品或其他目标产品的组合进行集成。针对集成交付中产生的流程、决策、假设、异常、纠正行动、经验总结等完成归档。
- 对于交付给最终用户的情况，目标产品安装在相应的场站；相应的验收与鉴定工作完成；用户、操作人员、维护人员及其他相关人员的培训已经完成；取得验收文档之后，交付工作结束。
- 所有已实现的辅助产品也相应完成交付，包括交付辅助产品产生的技术规程、决策、假设、异常、纠正行动、经验总结等。

5.5.2 产品交付指南

5.5.2.1 产品交付输入需要考虑的附加信息

在评价输入对成功实现产品交付流程是否必要时，考虑所有客户和利益相关者，并考虑技术上、工程上及安全性的需求非常重要。其内容如下所述。

- **运输性需求：**如果需要，本项需求用于定义所关注系统运输方面的技术状态需求。或者说，本项需求细化为运输系统产品所需的外部系统，以及与这些系统的接口。
- **环境方面的需求：**本项需求用于定义所关注系统在交付（包括系统的存储和运输）过程中需要的环境条件。
- **维护性需求：**本项需求细化所关注系统需要的维护频率、维护人员和维护手段（必要时还包括注意事项和保障条件）。

- **安全性需求：**本项需求用于定义所关注系统的寿命周期安全性需求，以及与安全相应的设备、设施、人员需求。
- **保密性需求：**本项需求针对所关注系统定义信息技术需求，国内交付和国际出口的保密安全需求，以及实物安全需求。
- **工程性需求：**本项需求用于定义成本与进度方面的需求。

5.5.2.2 产品交付最终用户后——做什么？

本手册的第2章中曾提及，产品交付给最终用户之后进行的活动与系统工程引擎之间有关系。如图2.3-8所示，在产品部署到最终用户之后，在其使用、管理、维护中持续发挥系统工程功能。在这些活动中可以应用第6章描述的技术管理流程。任何时候如果需要新的能力、产品升级或者辅助产品，系统工程的开发流程将再次执行。当产品完成使命之后，将执行寿命周期早期开发的退役、处置或淘汰计划。

第 6 章 技术管理

本章介绍图 2.1-1 技术管理流程中的活动，并且按照图 2.1-1 中列出的步骤 10~步骤 17 划分小节。每个步骤中流程的输入、活动和输出都进行讨论。并提供与 NASA 项目相关的实例作为指南补充部分。

技术管理流程是项目管理和技术开发团队之间的纽带。在引擎的技术管理部分，8 个相互关联的流程提供了相关功能的集成，从而能够实现设计方案。尽管不是每个技术团队成员都直接参与这 8 个流程，但是他们却间接受到这些关键功能的影响。技术团队的每个成员都依赖于技术规划、需求管理、接口管理、技术风险管理、技术状态管理、技术数据管理、技术评估、决策分析来满足项目目标。没有这些相互关联流程，单个成员和任务就不能集成到在费用和进度约束范围内满足运行使用构想的功能系统中。工程管理团队在分配的任务中使用相互关联功能来实施项目控制。

这些工作从技术团队在 A 前阶段进行大量规划时开始。有了这些早期详细的控制基线计划，技术团队成员将理解所有团队成员的作用和职责，并且项目将能够确定工程费用和进度目标。通过这些工作，开发并确立系统工程管理计划。一旦确立了系统工程管理计划，它必须与项目主计划和进度表同步。另外，确立和执行所有技术合同工作的计划也同时明确。

这是一个递归迭代的过程。在寿命周期早期，建立计划并与设计和实现流程同步。随着系统在寿命周期中的成熟和进展，这些计划必须更新以反映当时的环境和资源，并控制项目性能、费用和进度。至少，这些更新将在每个关键决策点发生。然而，如果项目有显著的变更，如利益相关者期望更新、资源调整或其他约束，就必须针对所有计划变更对标定项目的影响进行分析。

下面各节将逐一介绍 8 个技术管理流程及其针对给定 NASA 使命任务的相应产品。

相互关联技术管理的关键点

- 通过开发作为技术规划基础的技术产品分解结构、技术进度表和工作流程图、技术资源需求和约束（资金、预算、设施和长期事项），完整理解并规划技术工作的范围。
- 定义所有接口并指派每个组织内部和组织之间的接口授权和责任。这包括理解潜在的不兼容性并定义转换流程。
- 技术状态控制对于理解变更如何影响系统是关键的。例如，设计和环境的变更可能导致先前的分析结果无效。
- 进行里程碑评审，保证关键并且有价值的评估。这些评审的动机不是用于满足合同或进度。这些评审有特定的启动准则，当满足这些准则时可以进行评审。
- 了解任何影响分析结果的偏见、假设和约束。
- 将所有分析置于技术状态控制之下，能够追踪变更的影响并了解何时需要重新进行评估分析。

6.1 技术规划

技术规划流程是系统工程引擎中包含的 8 个技术管理流程的第一个，它为应用和管理每

个公共技术流程确立一个计划,这个计划将能够用来驱动系统产品和相应工作产品的开发。这个流程还为辨别和定义技术工作确立一个规划,这些技术工作是在项目费用、进度和风险约束下为满足项目目标和寿命周期成功准则所必要的。

6.1.1 流程描述

图 6.1-1 所示是技术规划流程一个典型的流程图并且给出了技术规划中需要考虑的典型输入、输出和活动。

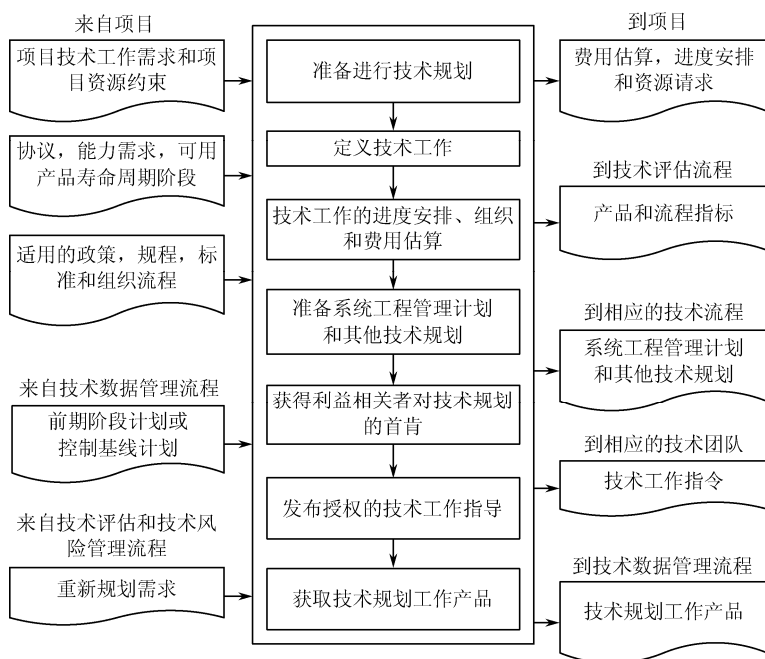


图 6.1-1 技术规划流程

6.1.1.1 输入

技术规划流程的输入来自工程管理和技术团队,或来自其他公共技术流程的输出。基于技术性和工程性需求、约束、政策和流程,初步规划利用来自项目外部的输入确定技术工作的整体范围和框架。在项目的整个寿命周期,技术团队持续将系统工程引擎其他流程生成的或来自项目指定需求和约束的决策和评估结果纳入技术规划策略和文档,以及所有内部变更中。

随着项目在寿命周期各阶段的进展,对每个后续阶段的技术规划必须进行评估并不断更新。当项目从寿命周期一个阶段转入下一个阶段,对即将进入的寿命周期阶段的技术规划必须进行评估和更新,以反映出最新的项目数据。

1. 来自项目外部的输入

项目计划提供了项目的顶层技术需求,包括工程分派给项目的可行预算,以及保证工程整体需要的项目进度表。尽管分配给项目的预算和进度将作为项目的约束,技术团队仍需依据满足项目技术需求所需的实际工作制定一个费用估算和进度安排表。在项目的寿命周期内,项目分配预算和进度与技术团队实际费用估算和进度安排之间的差异都必须持续地协调一致。

项目计划同时还定义了适当的项目寿命周期阶段和里程碑，以及项目成功实施所需要的外部 and 内部协定或者能力需求。项目寿命周期阶段和规划的里程碑将为确立技术规划工作和生成满足全部项目里程碑所需的详细技术活动和产品提供整体框架。

最终，项目规划还包括在执行技术工作过程中必须遵循的所有与规划相关的政策、技术规程、标准和组织流程。技术团队必须开发相关技术途径保证项目需求得到满足，保证在开发中间产品和目标产品时使用的任何技术规程、流程和标准都遵从项目计划中指定的政策和流程。

2. 来自其他公共技术流程的内部输入

源自数据管理流程或技术状态管理流程（控制基线明确或来自寿命周期前一阶段）的最新技术规划应该用于寿命周期下一阶段的技术规划更新。技术规划可能需要更新，这主要基于技术评估流程中进行的技术评审、技术风险管理流程中确认的问题或者是决策分析流程中做出的决策。

6.1.1.2 流程活动

鉴于技术规划与 NASA 系统工程相关，其任务是确认、定义和规划 NPR 7123.1 《NASA 系统工程流程和需求》中的 17 项公共技术流程如何在寿命周期各个阶段中应用于系统结构内部的工作分解结构模型所有层次，从而满足产品寿命周期成功准则。该流程形成的关键文档是系统工程管理计划。

系统工程管理计划对项目规划来说是一个附属文档。系统工程管理计划对所有项目参与人员定义了确定的项目约束下如何进行项目技术管理，工程规划定义了确定的规划约束下为达到目标如何进行项目管理。系统工程管理计划同时还说明了在项目寿命周期的各个阶段如何应用系统工程技术。

技术规划应当与技术风险管理流程（参见 6.4 节）和技术评估流程（参见 6.7 节）紧密地结合在一起，确保针对项目中已明确的问题，未来活动由正确行动构成。

相比于工程计划或项目计划，技术规划专注于系统产品开发需要的技术工作范围。项目负责人专注于整个项目寿命周期的管理，而由系统工程师领导的技术团队则专注于项目技术方面的管理。在安排和组织适当的并行工程时，技术团队负责确认、定义并开发实施系统分解、定义、集成、验证和确认的计划。其他计划还包括定义和规划适当的技术评审、审核、评估，提出状态报告，并确定所有专业领域工程技术和设计验证需求。

本节描述如何实施图 6.1-1 所示的技术规划流程中包含的活动。在项目开始时做出的初始技术规划将确定技术团队成员、明确团队成员的作用和职责，以及开展技术工作过程中将要使用的工具、流程和资源。另外，技术团队期望实施的活动及其相应生产的产品将会被明确、定义和安排进度。在获取所完成任务的实际数据并且已知近期和未来活动细节的情况下，技术规划将持续演化发展。

1. 技术规划准备

为了能够正确进行技术规划，执行技术规划的流程和技术规程应该辨识、定义和说明。对参与者进行确认时，其作用和职责，以及任何训练和认证活动将被清晰的定义和说明。一旦这些流程、人员、作用和职责都就绪，应该为技术工作制定一个规划策略。一个基本的技术规划策略应该考虑的事项如下：

- 系统工程管理计划所需，以及其他所有技术规划文档所需要的规划文档层次；
- 确定和收集输入文档；
- 将要开展的技术工作序列，包括输入和输出；
- 来自技术工作的可交付产品；
- 如何获取技术活动的工作产品；
- 如何辨识和管理技术风险；
- 执行技术工作所需要的工具、方法和培训；
- 利益相关者在技术工作各个方面的投入；
- NASA 技术团队将如何与外部承包商的技术工作保持密切联系；
- 里程碑和成功准则，如技术评审和寿命周期阶段；
- 内部接口和外部接口的辨识、定义与控制；
- 相关经验教训的总结并加入到技术规划中；
- 用于技术开发的途径和如何将技术开发的成果加入到项目之中；
- 辨识和定义用于度量已实现产品和跟踪技术进展的技术衡量指标；
- 做出进行制造、购买和重用决策的准则，以及商业现货供应软件和硬件的加入准则；
- 辨识和缓解非常规性能的计划；
- 应急计划和重新规划的基础指导；
- 状况评估和报告的计划；
- 决策分析的方法，包括需要的材料、需要的技能，以及对精度的期望。

考虑项目的上述事项和其他特点，技术团队将拥有一个理解和定义技术工作范围的基础，包括通过全面技术工作能够得到的可交付产品，技术团队必须保障项目进度表和关键里程碑，同时保障技术团队为完成工作所需要的资源。

定义技术规划工作中一个关键因素就是了解与进行辨识活动相关的工作量。一旦结合考虑技术工作的范围，技术团队能够开始着手定义特定的规划活动，估计完成每项任务所需要的工作量和资源。从历史经验来看，许多项目都低估了完成适当规划活动所需要的资源，并且为了跟上项目中的变更而被迫进入一种连续危机管理的状况。

2. 定义技术工作

技术工作必须被完全定义。在开展技术规划时，应当使用费用、进度和劳动资源的实际价值。无论是从历史数据中推断得来，还是从与项目和利益相关者的交互规划进程中得来，必须计算实际价值并提供给项目团队。任何估计中都应该包含基于工作的复杂程度和危险程度的偶然事件。必须制定应急计划。应急计划的例子如下：

- 在硬件和系统的开发和测试过程中，需要额外的、计划外的软件工程资源来辅助故障/异常检测。软件工程师经常被召唤来帮助检测故障问题并准确定位硬件及系统开发和测试中的错误源（如编写附加测试驱动程序来调试硬件问题）。为了适应不可避免的组件和系统调试，避免费用超支和进度延迟，更多的软件人员应该列入项目的应急计划之中。
- 在技术规划的应急计划之中必须考虑硬件在回路问题。硬件在回路测试是一个典型的调试试验，其中硬件和软件首次集中在硬件在回路的昂贵环境里。如果理解试验期间出现的信息和错误这项前期工作没有完成，硬件在回路设备上耗费的额外时间将可能导致可观的费用和进度影响。这些影响可以通过前期规划来减轻，例如，在试验前为技术团队提供合适的调试软件等。

3. 技术工作的进度安排、组织和费用

一旦技术团队定义了需完成的技术工作，工作的焦点就集中在对项目的技术部分进行进度安排和费用估算。技术团队必须参照项目的工作分解结构，以事件的逻辑顺序组织技术任务，考虑主要的项目里程碑、分段计划可用预算，并安排保障资源可用时间。

1) 进度安排

在工作分解结构中描述的产品来自于需要花费时间完成的活动。这些活动之间有时间先后关系，这种关系可以用来创建一个网络化进度表，明确定义活动之间的依赖关系、资源的可用性及来源于外部的资源。

进度安排是项目行动规划和管理的重要组成部分。创建网络化进度表的过程定义和表达“需要做什么”、“这么做持续多长时间”，以及“项目工作分解结构的各个元素之间如何影响”。一个完整的网络化进度表可能被用来计算完成项目需要多长时间，哪些活动决定项目时间（即关键路径活动），以及项目的其他活动有多少富余（备用）时间。

“关键路径”是一组相互依赖的任务序列，决定完成项目需要的最长持续时间。这些任务决定进度并且持续变化，因而必须不断更新。这条关键路径可能包含一个任务或者一系列相互关联的任务。如果项目需要在资源约束下按时完成，确认关键路径和为完成关键路径中的关键任务所需要的资源是非常重要的。随着项目的进展，关键路径会随着关键任务的完成或其他任务的延误而改变。不断演变的具有明确任务的关键路径需要在项目推进过程中仔细监控。

网络化进度安排系统帮助项目负责人精确评估技术和资源变化对费用和进度的影响。费用和技术问题经常首先以进度问题显现出来。了解项目的进度对确定精确的项目预算和跟踪项目性能和进展来说是一个前提。因为网络化进度表显示出每个行动如何影响其他行动，可以辅助评估和预测项目进度的前移结果或整个项目中某个活动的加快程度。

2) 网络化进度表数据和图形格式

网络化进度表数据如下：

- 活动和相关的任务；
- 活动间的依存关系（如某个活动必须依赖于另一个活动才能被接受）；
- 作为一个或者多个活动结果的产品或者里程碑；
- 每项活动的持续时间。

网络化进度表包含了以上所有四个数据项。当创建网络化进度表时，创建这些数据元素的图形格式可能是规划和组织进度表数据的良好起步。

3) 工作流图

工作流图是上述前三个数据项的图形显示。图 6.1-2 所示的是两个通用类型的图形格式。一种是活动有向图，箭头的起始端和终止端表示活动产品及属性。这是工程计划网络评审技术图（PERT）的典型格式。

第二种格式，称为顺序图，使用方框代表活动，而用箭头表示活动的属性。顺序图格式允许的逻辑关系的简单描述如下：

- 活动 B 在活动 A 开始时开始（SS）；
- 活动 B 仅在活动 A 结束后开始（FS）；
- 活动 B 在活动 A 结束时结束（FF）。

这三个活动关系的任何一个都可以通过附加一个时间区间（用符号+或-表示）来进行修正，如图 6.1-2 所示。在顺序图中可以将若干个低层次活动概括成为一个概要活动并与一个简单活动关联。如针对最开始的低层活动，可以通过“开始即开始”关系将一个概要活动与之关联。然后将这个概要活动通过“结束即开始”关系与最后的低层活动关联。在顺序图中最常用的关系是“结束即开始”关系。箭头表示活动的格式在需要时能够通过创建人工事件和活动以顺序图形式表示时间先后逻辑。

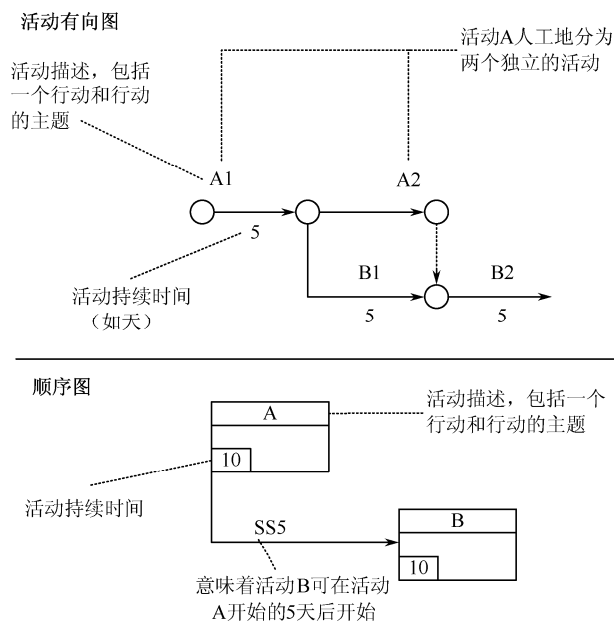


图 6.1-2 网络化进度表活动有向图和顺序图

4) 建立一个网络化进度表

进度安排以确定工作分解结构顶层所描述产品的项目层目标进度开始。为了开发与项目目标一致的网络化进度表，以下 6 个步骤需应用到工作分解结构最低可用层次的每个单元。

第 1 步：明确完成每个工作分解结构单元所需要的活动和属性。必须明确足够的活动来精确定显示活动与其他工作分解结构单元之间的进度依赖关系。第 1 步最容易完成，如下所述。

- 确保工作分解结构模型向下扩展而能描述所有的重要产品，包括文件、报告，以及硬件和软件产品。
- 对每个产品，列出其产生所需要的步骤并使用流程图绘制流程。
- 表示产品之间的依赖关系，以及全部工作中的所有集成和验证步骤。

第 2 步：辨识和议定外部依赖关系。对工作分解结构单元而言，外部依赖关系即任何来自外部的接收件，以及任何向外交付的单元产品。应当进行产品评议，确保其内容、格式和标签方面意见一致，从而低层的进度安排能够被集成。

第 3 步：估算所有活动的持续时间。应当记录这些估算的假设基础（员工队伍、设施的能力等），以备未来的引用。

第 4 步：将每个工作分解结构单元的相关数据输入到一个进度安排程序，获取其网络化进程表和针对该单元关键路径的估算。通常可以通过步骤 1~步骤 4 的某种迭代获得满意的进度安排表。在关键路径活动中经常增加储备，从而保证在限定的风险等级内满足进度安排的约定。

第 5 步：集成低层工作分解结构单元的进度表，从而单元之间的所有依赖关系能够正确

地包含在项目网络中。在此加入假期、周末等时间的影响是非常重要的。在这一步最终形成项目的关键路径流程。

第6步：随时评审员工队伍水平和资金状况，并对逻辑顺序和持续时间做出最终调整，从而保证员工队伍水平和资金水平在工程约束之内。

对活动逻辑顺序和持续时间的调整可能需要与项目层建立的进度目标相吻合。活动调整可能包括给某些工作分解结构单元添加更多活动，删除冗余活动，给关键路径上的某些活动增加员工，或者设法以并行方式而非串行方式开展更多活动。

此外，好的做法是保留或者备份某些进度表，作为风险缓解战略的一部分。以上最后几个步骤的产品是个工作分解结构单元与所有其他工作分解结构单元活动之间一致的可行的进度表控制基线。所有进度表应该与项目的技术范围和进度目标一致。在集成的主进度表中应该有足够的余量，从而保证进度和相关费用风险能够被项目主管和客户接受。即使做到了这些，由于接收件的延迟到达，可能造成许多工作分解结构单元的时间估计不足或某些工作分解结构单元的工作不能尽早开始。此时，几乎需要重新规划来满足项目目标。

5) 表述技巧

关于进度表的概要数据经常以图表方式描述。甘特图是使用项目工作分解结构中产品单元的的开始和结束日期描述项目进度的线条图。某些甘特图还能显示活动之间的依赖关系（如先后顺序和关键路径）及当前状态。图 6.1-3 所示的是甘特图示例（参见关于甘特图特点的注记）。

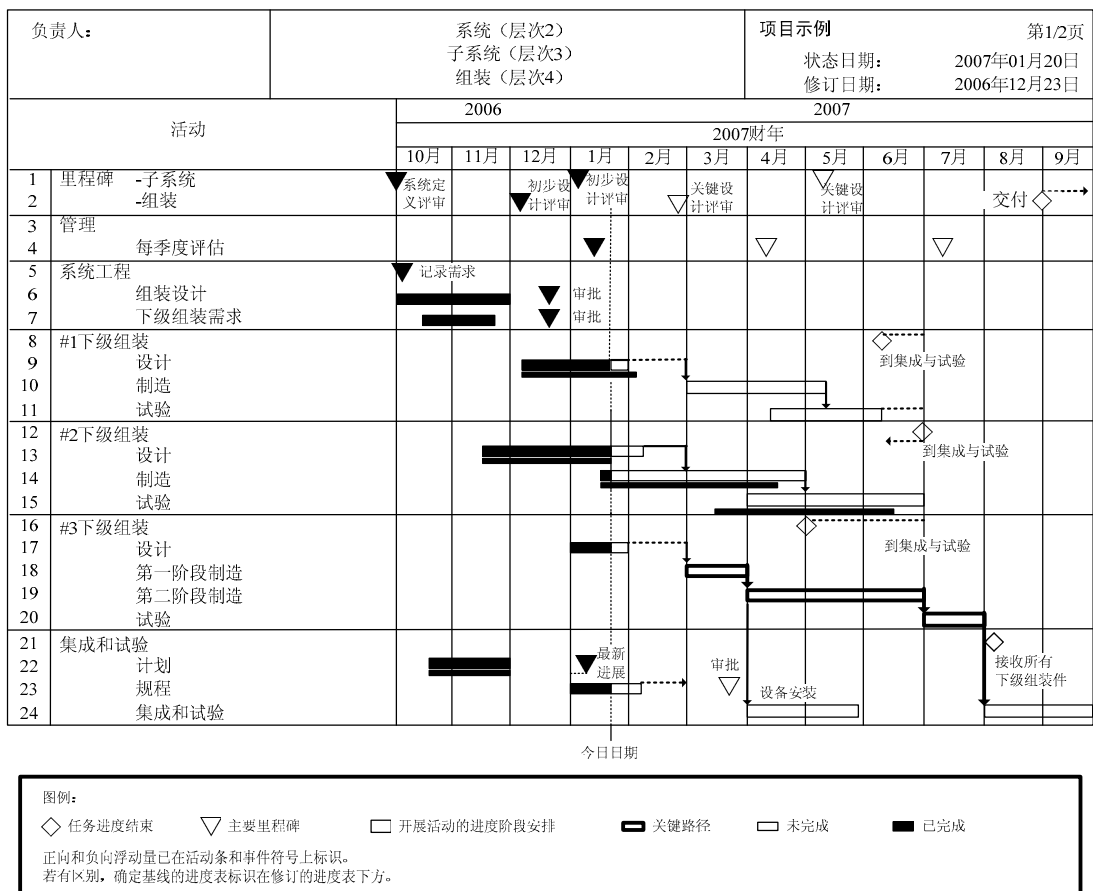


图 6.1-3 甘特图示例

另一种类型的输出格式是显示关键活动余量和近期变化的表格。例如，项目负责人可能希望精确知道进度表保留的时间被关键路径活动消耗的程度，进度表保留的时间是否正被消耗或被保留到最终阶段。这个表格提供了关于进度表保留时间变化率的信息。

甘特图特点

图 6.1-3 所示的甘特图说明了下列可用的特点。

- 标题，描述工作分解结构单元，确认责任人，并且提供使用进度表控制基线的日期，报告进度表状态的日期。
- 进度表主体中的里程碑阶段（第 1 行和第 2 行）。
- 进度表主体中的活动部分。显示的活动数据如下：
 - 工作分解结构单元（第 3, 5, 8, 12, 16 和 21 行）；
 - 活动（从工作分解结构单元获取）；
 - 当前计划（以粗线条表示）；
 - 控制基线计划（与当前计划一样，如果不同，将以粗线条后面的细线条表示）；
 - 每个活动的余量（里程碑之前水平虚线，第 12 行）；
 - 进度对控制基线偏差（当前计划线后的水平虚线）；
 - 关键路径，在第 18 行~第 21 行显示，影响第 24 行；
 - 在状态报告日期的状态线（从图表主体的顶部贯穿底部的竖直虚线）。
- 一个说明图表中符号的图例。

这个甘特图只显示了 24 行，这些行表示的是本工作分解结构单元中当前正在进行的活动概要。在进行项目状态报告时，将报告裁剪为最相关的细节内容是恰当的。

6) 资源平衡

好的进度安排系统提供了显示不同时间上资源需求，以及进行调整的能力，使得进度表针对不同时间上资源约束是可行的。资源可能包括员工水平、资金状况、重要设备等。目标是将浮动的任务开始日期移动到资源状况可行的时刻。如果这还不够，则需要重新检查对造成资源紧张的活动所假设的任务持续时间，并且相应改变资源水平。

7) 预算编制

预算编制和资源规划包括建立一个合理的项目控制基线预算，形成对由技术和/或进度引起的控制基线变化的分析能力。项目的工作分解结构、控制基线进度表和预算应该视为相互依赖的，反映满足工程目的和目标的技术内容、时间和费用。预算编制过程应考虑是否存在一个固定的成本上限或成本计划。当不存在这样的上限或者计划时，需要从工作分解结构和网络化进度表中开发一个控制基线预算。其中需要特别考虑员工和其他资源需求，以及考虑劳动力价格和其他财政及规划因素的结合来获得成本要素估算。这些成本要素如下：

- 直接劳动成本；
- 间接成本；
- 其他直接成本（旅行、数据处理等）；
- 分包合同成本；
- 材料成本；
- 行政和管理成本；
- 资金成本（即可能支付的利息）；
- 薪水（如果需要）；
- 应急开支。

当存在成本上限或者固定成本计划时，就有在完成预算和规划流程之前必须满足的更多

的逻辑门。需要确定工作分解结构和网络化进度表对于指定的成本上限和/或开支计划是否可行。如果不可行,就需要考虑延长项目(通常在总成本增加时)或者缩小工程的目标和目的、需求、设计和实施方法的范围。

如果存在成本上限或者固定成本计划,当它们的控制基线划定后控制开支就很重要了。开支控制的一个重要方面是项目开支和进度状态的报告和评估,相应的方法在 6.7 节讨论。另一个方面是开支和进度风险规划,例如,开发风险规避和替代策略。在项目层次,预算编制和资源规划必须确保有充分的应急资金用于应对不可预见的事件。

寿命周期费用估计的成熟度应做如下推进。

- **A 前阶段:** 初始寿命周期费用估算(70%置信水平,显然要考虑较多的不确定性);
- **阶段 A:** 寿命周期费用估计初步审批;
- **阶段 B:** 批准寿命周期费用估计(初步审计评审时达到 70%置信水平);
- **阶段 C、阶段 D 和阶段 E:** 使用挣值管理报告寿命周期费用估计偏差并更新寿命周期费用估计。

如果出现以下情况,费用估算的可信水平就值得怀疑。

- 工作分解结构费用估算仅能用美元而不能用其他计量单位表达,这说明没有充分定义辨识流程和资源的需求。
- 估算的基础没有包含对工作范围和估算成本(及进度)合理性独立验证的充分细节。
- 实际开支与寿命周期费用估计相比有明显不同。
- 开展的工作没有初始规划,导致开支和进度偏差。
- 进度和费用挣值趋势明显表明不容乐观的性能。

4. 准备系统工程管理计划和其他技术规划

系统工程管理计划是项目主要的和顶层的技术管理文件,在规划论证阶段的早期开发,并且在整个项目寿命周期内更新。系统工程管理计划由项目的类型、项目寿命周期的阶段,以及技术开发风险作为驱动因素,并针对每个项目和项目单元制定。系统工程管理计划的特定内容根据项目裁剪,其中推荐的内容在附录 J 中讨论。

在整个项目规划下工作的技术团队,根据需要开发并更新系统工程管理计划。技术团队与项目负责人一起工作,评审其中内容并取得一致。其中,允许对设定的技术活动如何影响项目的规划、费用和进度方面进行彻底地讨论和协调。系统工程管理计划提供技术工作的细节,并且描述需应用哪些技术流程,如何采用适当的活动应用这些流程,如何组织项目来完成这些活动,以及完成这些活动相关的费用和进度。

系统工程管理计划的文字长度并不是重要所在。每个项目都有不同的重要之处。计划必须适当考虑项目的具体技术需求。系统工程管理计划是一个根据需要不断更新变动的文件,在项目实施过程中,一旦开发出新的可用信息便加入其中。系统工程管理计划不能复制其他项目文件,但是系统工程管理计划应该参考和概括其他技术规划的内容。

系统工程师和项目负责人必须基于项目的范围和类型辨识需要附加的技术规划。如果规划没有包含在系统工程管理计划内,就应该在开发系统工程管理计划时引用和协调。其他规划,如系统安全性和风险概率评估,同样需要规划,并与系统工程管理计划协调。如果一个技术规划是独立的,它应该在系统工程管理计划中引用。根据项目的规模和复杂性,这些规划可能是独立的或包含在系统工程管理计划之中。一旦确定,即可开发技术规划,进行规划培训,并且实施规划。系统工程管理计划之外的附加技术规划示例在附录 K 中给出。

系统工程管理计划必须与项目规划同时开发。在开发系统工程管理计划的过程中,项目的技术方法,以及项目寿命周期的技术方法同时被开发,这决定了项目的持续时间和费用。工程性和技术性管理方法的开发要求项目关键人员了解待开展的工作和工作各个部分之间的关系。分别参见 6.1.2.1 和 6.1.1.2 节关于工作分解结构和网络化进度表的论述。

系统工程管理计划的开发需要来自于所有能显著影响项目结果的领域中规划方面和技术方面知识渊博专家的贡献。建立一个项目负责人信任的和保证项目团队全部投入的系统工程管理计划需要有知名专家的参与。

系统工程管理计划的作用

系统工程管理计划是一个规则书,它对所有参与者描述了如何进行项目的技术管理。负责项目的 NASA 中心应该有一个系统工程管理计划描述它将如何实施技术管理,并且每个承包商应该有一个系统工程管理计划描述如何依照合同和 NASA 的技术管理惯例实施管理。与项目密切联系的每个中心都应该对其负责的项目部分有一个系统工程管理计划,与负责项目的 NASA 中心系统工程管理计划交互,而这个较低等级的系统工程管理计划具体考虑本中心的技术工作及如何与整个项目交互。鉴于系统工程管理计划是项目唯一和合同唯一的,它必须在每个显著的工程性变更发生时进行更新,否则,它将变得过时和无用,项目将陷入无法控制的状态。负责的 NASA 中心应该在准备进行初始费用估算之前开发出系统工程管理计划,因为那些引起开支的活动(如技术风险缩减)需要事先确定和描述。承包商应该在项目申请时(确定费用和价格之前)就开发完系统工程管理计划,描述项目的技术内容、可能昂贵的风险管理活动和所用的确认和验证技术,这些必须包含在项目费用估算的准备工作中。相关 NASA 中心的系统工程管理计划应该伴随项目主系统工程管理计划开发。项目系统工程管理计划是项目的高级技术管理文档,所有其他技术规划必须服从它。系统工程管理计划应该是全面的综合的,并且描述全局工作将如何被管理和实施。

5. 获得利益相关者对技术规划的认同

为了获得利益相关者对技术规划的认同,技术团队应该保证利益相关者有办法针对其利益的实现提出看法,并评审项目规划。在论证阶段,利益相关者的作用应该在项目规划和系统工程管理计划之中定义。规划的评审和利益相关者对规划内容的认同构成利益相关者在技术方法方面的实际控制权。在项目寿命周期该阶段的后期,利益相关者负责将其结论发送给项目。关于利益相关者责任的初步协议对保证项目技术团队获取利益相关者的审批结论很关键。

明确利益相关者是系统工程过程的一个早期步骤。随着项目的进展,利益相关者的期望伴随逻辑分解流程向下细化,如此明确所有主要的和派生的需求所对应的利益相关者。利益相关者参与是技术需求定义的一个关键部分。随着需求和运行使用构想的开发,需要利益相关者对这些产品的认同。不当的利益相关者参与将导致不合适的需求,并且导致产品不能达到利益相关者的期望。相应的利益相关者参与状况应该被追踪,如果利益相关者没有按照计划参与,就应该采取校正行动。

在项目寿命周期全过程中,与利益相关者的交流和来自利益相关者的审批可以通过协议完成。工程组织可以使用一个内部任务协议,一个谅解备忘录,或者其他相似文档来确立项目和利益相关者之间的关系。协议还用来在定义待交付产品时记录相关客户和供应商的责任。这些协议应该确立效能指标或性能指标,效能指标和性能指标被用来监控活动的进展。对报

告的需求和进度的需求都应该在这些协议中确立。这些协议的准备将保证利益相关者的作用和责任支持项目目标，且项目有办法处理辨识出的风险和问题。

在项目规划和系统工程管理计划的开发过程中，建立项目寿命周期内专门的讨论制度便于交流和记录决议。这些讨论制度包括会议、工作小组、决策小组和控制委员会。每个讨论团体应该确立一个纲领来定义所讨论的范围和管辖权，并且确定必要的有投票权和无投票权参与者。在处理特别议题时，如果需要专门知识和特定利益相关者的意见，则需要确定特别参与者。要确保已经确定的利益相关者对讨论的支持。

6. 发布技术工作指南

技术团队向成本账目管理员提供技术工作指南。这使得成本账目管理员能够准备详细的规划，从而相互一致并共同开展所有相关工作。这些规划包括详细的进度和需要进行费用管理和挣值管理的成本账目预算。

当需要一个详细规划控制基线时，发布技术工作指南是项目阶段 B 的一项重要活动。如果这个活动没有进行，成本账目管理员将缺乏足够的指导来进行详细规划。挣值管理需要的进度和预算将会基于假设和项目级信息的局部解释。如果真是这种情况，那么将很有可能在控制基线规划和已开展工作之间产生重大差异。为成本账目管理员提供技术工作指南能够形成一个更加组织化的技术团队。这项活动在进行重新规划时可能要重复进行。

这项活动不限于系统工程。只要有对精确控制基线规划的需求，这项活动就是项目规划的一个正常部分。技术团队将针对工作分解结构的系统工程单元内每个成本账目为成本账目管理员提供技术指南。这些指南可以采用任何格式，但应对每个账目清晰交流以下信息：

- 期望的技术产品；
- 对每个成本账目的文献和技术报告要求；
- 关键事件和支持该事件的特殊成本账目管理员所期待的特定产品（如期待开支账目在初步设计评审的特定议题中提供演示）；
- 对可用要求、政策和标准的引用；
- 鉴别需使用的特定工具；
- 在进入项目管理之前，对技术团队如何协调和评审成本账目规划的说明；
- 关于工作如何开展和由谁来实施所制定的决策。

成本账目管理员接受这些技术指南及项目规划指南，并准备成本账目计划。这些计划可以采用任何格式并且在不同中心使用不同名字，但是至少应该包括以下内容。

(1) 成本账目的范围包括如下内容。

- 待交付的技术产品；
- 为完成交付件需要开发的其他产品（如可能需要开发技术状态管理系统以便交付“管理中的技术状态”这项产品）；
- 关于技术规程的概要描述，按照这个技术规程来完成相关产品的工作，例如：
 - 产品 X 将在内部准备，使用局部技术规程 A，该技术规程在组织 ABC 中普遍使用；
 - 产品 X 将以下列方式验证/确认……；
 - 产品 X 将以下列方式交付到项目……；

- 产品 X 的交付将包含以下报告（如交付到项目的技术状态管理系统包括技术状态状况的常规报告等）；
- 产品 Y 将按照购买技术规程 B 购置。

(2) 一个隶属于该规划的进度表，采用与项目进度指南相适应的格式。这个进度表应当包含上面提到的每个技术规程和交付件，并且为每个技术规程的活动步骤提供附加信息。

(3) 一个隶属于该规划的预算，采用与项目预算指南相适应的体制。这个预算与进度安排的活动所需资源相一致。

(4) 任何必要的协议和审批手续。

如果项目预备使用挣值管理，那么成本账目的范围内需要进一步确定大量“工作包”，这些工作包是一些能够安排进度和估算费用的工作单元。工作包应该最大限度基于已完成的产品，也可能基于已经完成的技术规程（如完成的确认流程）。每个工作包都有自身的进度和预算。工作包预算成为挣值管理系统中工作计划预算（BCWS）的一部分。当工作单元完成时，项目赚取相应的价值增加量。在成本账目中可能还有一些未完成工作，这些工作还不足以定义为一个工作包集合。例如，启动运行将得到技术团队支持，但是关于“将要做什么”的细节经常在阶段 B 中还没有解决。在这种情况下，这些未完成的工作又称“计划包”，它拥有高层次进度表和全局预算。当这些工作被更好地了解时，这个计划包将分解成工作包，从而挣值管理系统能够继续在启动运行时的执行。

成本账目计划应该得到技术团队和成本账目管理员所在组织中产品系列管理者的评审和认可。计划指南可以确定附加的评审和审批需求。

以上描述的规划流程不限于系统工程。对飞行项目而言这是所有单元应该实施的流程。系统工程师在规划中可能起到的作用是证实在成本账目计划中描述的项目工作范围与项目工作分解结构字典相一致，并且这个工作分解结构字典与项目的架构相一致。

7. 获取技术规划工作产品

技术规划流程的工作产品应该使用技术数据管理流程或者技术状态管理流程进行管理。技术规划中一些更为重要的产品（如工作分解结构、系统工程管理计划和进度表）都在技术状态管理控制之下，并且通过技术状态管理流程获取。技术数据管理流程被用来获取没有在正式技术状态管理控制下的权衡研究、成本估计、技术分析、报告和其他重要文件。工作产品，如会议记录和包含与利益相关者之间决策及协议的信函（包括电子邮件），应当保留并存入项目档案以备将来引用。

6.1.1.3 输出

技术规划活动的典型输出如下：

- 技术工作成本估计，进度表和资源需求，如在项目资源内的资金、劳动力、设施和（项目所用）设备。
- 评估技术工作进展和流程效率（用于技术评估流程）所需要的产品和流程度量指标。
- 支持技术工作实施的技术规划策略，工作分解结构，系统工程管理计划和其他技术规划（对所有流程，技术流程的可用规划）。
- 技术工作指南，如工作包或有工作授权的任务顺序（对相应的技术团队）。

- 需要用来提供流程活动的报告、记录和中间成果的技术规划流程工作产品（输出到技术数据管理流程）。

得到的技术规划策略应形成系统工程管理计划的一个轮廓或者草图。这作为初始准备完成之后整个技术规划流程的开始部分。当技术规划的准备完成后，技术团队就应该有一个技术规划工作的费用估算和进度表。支撑定义技术规划工作的预算和进度表可作为与项目负责人商谈的内容，在需要什么和可用什么的差异之间寻求解决方案。系统工程管理计划的控制基线需要完成。基于工程性变更的系统工程管理计划的更新规划需要开发和实施。系统工程管理计划需要经过适当层次权威部门的认可。

技术工作指南这一步骤产生成本账目管理员的规划指导，并产生一致的成本账目计划集。当需要挣值管理时，它产生挣值管理规划控制基线，包括工作安排预算费用。

6.1.2 技术规划指南

6.1.2.1 工作分解结构

工作分解结构是对完成项目所需开展工作的层次分解。工作分解结构是一个基于产品、可交付件和相关服务的层次划分。严格意义上来说，它需要包含项目的产品分解结构和特定的顶层主要产品，以及在依次降低的层次上的系统、部段、子系统等。最低层次的产品是硬件、软件和信息（文档、数据库等），这些产品有经认定的责任工程师和负责人。层次结构中的分枝节点应该显示产品分解结构单元是如何集成的。工作分解结构由产品分解结构及在产品分解结构每个分枝点加入任何必要的（管理、系统工程、集成和验证、综合后勤保障）服务单元构建而成。如果有多个工作分解结构单元需要类似设备或者软件（如系统保障设备），则可能需在系统层次定义更高层次工作分解结构单元来表示大宗采购或者开发活动。图 6.1-4 显示了系统、系统的产品分解结构和工作分解结构之间的关系。总的来说，工作分解结构是产品分解结构和系统层输入的组合。系统层的加入是为了保持与集成工作分解结构单元的一致性。

项目工作分解结构应该分解到与管理风险所对应的成本账目层。成本账目细化的适当层次由管理层对费用能见度的期望程度确定，根据成本的规划和报告进行权衡。承包商可以有一个合同工作分解结构，与他们控制成本的需求相适应。概要的合同工作分解结构，包括整个合同工作分解结构的上层，通常包含在项目工作分解结构中，向缔约的组织报告开支。工作分解结构单元应该以标题和系统序号标识，执行功能如下：

- 确定工作分解结构单元的层次；
- 确定能够集成较低层次工作分解结构单元的工作分解结构单元；
- 显示单元的成本账目。

工作分解结构应该拥有一个配套的工作分解结构字典，包含每个单元的名称、标识号、目标、描述，以及所有与其他工作分解结构单元相关的属性（如可接受性）。这个字典提供了一个结构化项目描述，这有益于引导项目成员和其他利益团体。它全面描述了每个工作分解结构单元期待的产品和服务。本节为开发工作分解结构提供了一些技术，并且指出一些需要避免的错误。

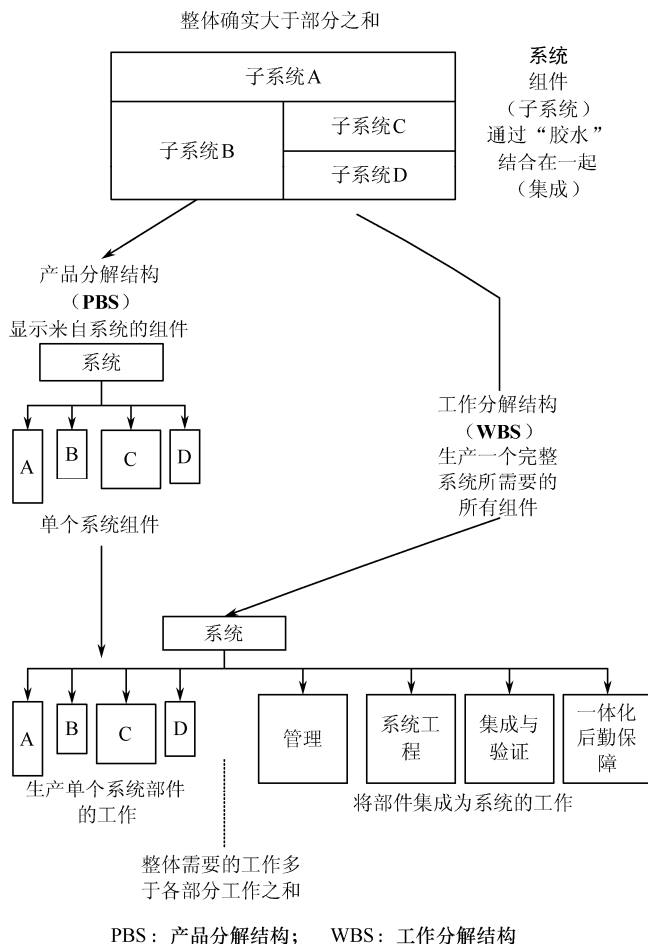


图 6.1-4 系统、产品分解结构和工作分解结构之间的关系

1. 工作分解结构的作用

技术团队应该接受来自项目办公室的规划指导。技术团队应该向项目办公室提供合适的系统工程工作分解结构单元的剪裁或扩展，并且在发布技术工作指导之前保证工作分解结构和工作分解结构字典在项目层相一致。

一个基于产品的工作分解结构的组织结构如下：

- 项目及技术规划和进度安排。
- 成本估算和预算制定（特别是在基于产品的工作分解结构中，可以通过与历史数据比较确定所考虑的费用。这是 DOD 工作分解结构标准的主要目标）。
- 定义合同工作规范和任务书范围。
- 项目状态报告，包括进度、开支、劳动力、技术性能，以及集成成本/进度数据（如项目挣值和估算成本）。
- 计划（如系统工程管理计划）和其他文档产品（如说明书和相关图纸）。

工作分解结构提供了一个描述整个项目的逻辑轮廓和词汇表，并且以连贯方式集成信息。如果在某个工作分解结构单元中增加了进度，观察者能够确定哪些其他工作分解结构单元最有可能被影响。费用影响需要更精确地估计。如果工作分解结构中的单元存在设计变更，

观察者能够确定哪些其他工作分解结构单元最有可能被影响，并针对潜在有害影响为这些单元提供咨询。

2. 开发工作分解结构的技术

开发一个成功的项目工作分解结构可能需要在项目寿命周期内的若干次反复迭代，因为全部可能的工作在开始时并不总是清晰的。开发初步工作分解结构之前，应该部分开发系统架构，直到能够生成初步的产品分解结构。这样产品分解结构和相应的工作分解结构将能够自上而下逐层地开发。在这个方法中，项目层系统工程师最终确定项目层产品分解结构，并且为较低层次提供产品分解结构草图。通过为低层添加适当的服务，如管理和系统工程，而得到工作分解结构。这个流程循环反复直到开发出期望的成本账目层的工作分解结构。另一个方法是在设计活动中定义完整产品分解结构的所有层次，然后开发完整的工作分解结构。在采用这个方法时，需要极度小心地开发产品分解结构，这样才能包含所有产品并且保证所有组装/集成验证分枝是正确的。建议那些负责较低层次工作分解结构单元的人员参与开发。

3. 开发工作分解结构过程中的常见错误

在工作分解结构开发中发现有三种常见错误。

- **错误 1:** 工作分解结构描述功能，不描述产品。这使得项目负责人成为唯一对产品正式负责的人。
- **错误 2:** 工作分解结构有分枝节点与工作分解结构单元的集成方式存在不一致。例如，在一个分布式体系结构的飞行操作系统中，通常软件及相关硬件需要在工作分解结构的相对较低层次被集成和验证。如果将它们视为在系统层集成的独立系统，而将软件和硬件分离是不合适的。这将导致在集成工作中难以指定责任，并且难以对系统部件集成和测试费用进行确认。
- **错误 3:** 工作分解结构与产品分解结构不一致。这可能导致产品分解结构不能完整的实行，并且通常造成管理过程复杂化。

这些错误的部分例子如图 6.1-5 所示。每个错误都将使得工作分解结构在项目规划和组织中无法充分发挥作用。通过使用上文描述的工作分解结构开发技术可以避免这些错误。

项目管理和系统工程学科共同之处是在一个系统化和结构化框架下，在系统寿命周期过程中系统管理和组织的需求反映将要开展的工作和相应的需要积累、总结和报告的费用、进度、技术和风险等数据（参见 NPR 7120.5）。

这个框架的关键部分是面向产品的层次化工作分解结构。来自物理和系统架构，工作分解结构提供系统的逻辑方法来定义和解释初始使命任务目标和技术概念，将它们转化为明确的项目目标、系统产品，以及寿命周期保障（辅助）功能。

若工作分解结构的结构适当，并且与合理的工程原理结合使用，能够为整个项目分解成明确定义的、面向产品的、逻辑关联的，并按层次、进度和相关责任排序的工作组件提供一个公共框架。

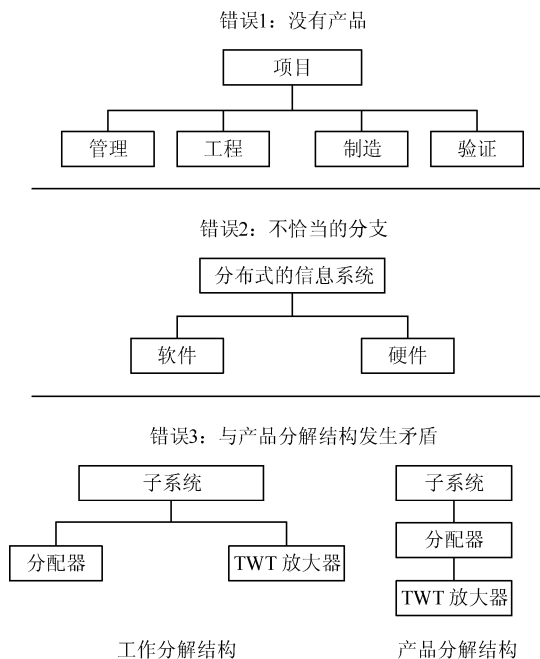


图 6.1-5 工作分解结构开发中错误示例

工作分解结构的层次结构和所需的详细程度由项目管理和技术团队确定，其依据是对项目的尺度和与技术工作相关的复杂性、约束、风险的仔细思考。初始工作分解结构将为工程/项目目标的概念化和定义，以及将初始概念转化为待开发、生产和获取的主要系统、组件产品和服务提供结构框架。随着逐层细节被定义，工作分解结构的层次结构将形成反映项目的全部工作，以及在项目的整个寿命周期需实现的每个系统或者目标产品的综合和完整视图。

主要交付产品分解到独立的明确的产品或服务单元，应当持续到能够表现每个工作分解结构单元如何被规划和管理的层次。不管是安排给内部组织或承包商，较低层次工作分解结构单元将被分解为附属的任务和活动，并聚集成工作包和控制账目，构成项目的费用计划、进度表和性能指标。

工作分解结构至少应该反映待开发和采购的主要系统产品和服务，辅助（支撑）产品和服务，以及任何位于结构低层的高开支和/或高风险产品单元。工作分解结构技术状态控制基线将作为项目规划的一部分归档，并用来构造系统工程管理计划。费用估算和工作分解结构字典的维护贯穿项目的全寿命周期，反映项目的当前范围。

论证审批文档、工程议定协议和工程/项目规划，这三个关键工程/项目文档的准备和批准对早期工作分解结构的开发起着显著的作用。

这些文档的初始内容将为感兴趣的工程确立意图、范围、目标和适当的协议，并列出经批准的项目、控制计划、管理方法，以及所有已经确认的约定和约束。

技术团队选择合适的系统设计流程，并应用到系统结构中自顶向下的每个产品定义之中。项目和系统结构分解为更小更易管理的组件，将为评估整个项目的完成情况和度量开支及进度情况提供逻辑要点。

系统的工作分解结构的层次结构

需要注意的是,实际上当面向产品时,NPR7120.5 指定的 NASA 空间飞行项目标准工作分解结构是从项目的角度而不是从系统的角度看待工作分解结构的开发。指定的工作分解结构反映了 NASA 主要项目的范围,因此,由项目常规寿命周期中多个主要系统开发、运行和处置构成。

NASA 空间飞行项目的工作分解结构层次结构包括高层系统产品(如有效载荷、空间飞行器和地面系统),以及辅助产品和服务(如项目管理、系统教育和教育培训)。这些标准产品单元已经确立并促进实施 NASA 的核算、采办和报告系统。

与 NPR7120.5 中描述的从项目视角开发的工作分解结构方法不同,技术工作分解结构的构建关注全部目标产品和在整个系统结构中作为低层单元的每个子产品的开发和实现。

NPR7123.1《NASA 系统工程流程和需求》为系统或目标产品的开发和实现指定了标准的系统化技术方法。使用模块构建方法或产品层次方法,系统架构逐层定义并分解成子系统(执行系统运行功能的单元)和相互关联的子单元(装配件、组件、部件及寿命周期辅助产品)。得到的层次结构或产品树描述产品分解结构中的整个系统架构。作为政府和工业界认可的“最佳实践”,产品分解结构的利用及其模块构建技术状态促进了 NPR7123.1 的 17 个通用技术流程在产品分解结构所有层次中的应用,也促进了系统层次结构中较低层次单元的逐层定义和实现。

产品分解结构的结构化定义和应用带来了一系列功能子产品或“子”工作分解结构模型。整个系统工作分解结构模型通过这些基于产品的子单元工作分解结构模型的逐层累积实现。

每个工作分解结构模型在全局系统技术状态中代表唯一单元或功能性目标产品,并且在将产品分解结构关联到单个模型的层次结构时,代表一个功能系统目标产品或“根”工作分解结构模型。

(参见 NPR7120.5《NASA 空间飞行工程和项目管理需求》)

一旦初始使命任务目标和目的演化成为待建系统或最终设计,工作分解结构将被细化和更新,从而反映项目的进展范围和架构,以及系统结构中自底向上每个产品的实现。在寿命周期的适当阶段,工作分解结构和工作分解结构字典将被更新以反映项目的当前范围并保证控制高风险和费用/进度问题。

6.1.2.2 费用定义和建模

本小节论述费用在系统分析和工程流程中的作用,如何度量它,如何控制它,以及如何对它进行估算。合理的开支及估算在系统工程中极其重要,体现了系统工程的主要目标:以效益最佳的方式实现系统的目标。每个备选方案的费用应该是系统工程流程中进行的权衡研究中最为重要的输出变量之一。

因此,费用估算的作用一个是帮助在备选方案中做出理性选择;另一个是在项目寿命周期中作为控制机制。项目寿命周期评审中,在确定系统目的和目标是否依然有效和可完成时,以及在确定约束和边界是否值得维护时,确定费用指标是非常重要的。这些指标在确定系统目的和目标是否已经适当地分解到各个子系统时同样很有用。

随着系统设计和运行使用构想的成熟,费用估算也随之成熟。每次评审中,都应该有费用估算,并且与看似能够完成项目的经费进行比较。必须特别注意早期评审中的费用估算,因为该项估算一般形成项目初始成本议定的基础。系统工程师必须能够为项目负责人提供实际的费用估算。如果没有这些估算,可能发生费用超支,并且整个系统内部和外部的开发流程的可信度将受到威胁。

1. 寿命周期费用和其他费用指标

为了在系统分析和工程中合理估算费用，许多问题需要考虑处理。这些问题如下：

- 应该计算哪些费用？
- 在不同时间发生的费用应该如何处理？
- 费用不能简单以货币单位度量应该如何处理？

1) 应当计算的费用

对备选方案费用最全面的度量指标是全寿命周期费用。根据 NPR 7120.5，系统的全寿命周期费用是“在项目的设计、开发、验证、生产、运行、维护、保障和处置期间，直接和非直接发生，重复和非重复出现，以及其他相关发生或估计将发生的费用。项目或系统的寿命周期费用还可定义为，从项目或系统的论证到实施完成整个寿命周期的全部费用。包括所有设计、开发、部署、运行维护及处置费用。”

2) 随时间发生的费用

寿命周期费用通常由若干年内的费用组成。为便于系统费用的工程权衡和比较，年度实际开支被换算为固定年度价值。这样排除了所有估算中通货膨胀的影响，并且可以直接进行备选方案比较。在那些主要进行投资组合架构分析的实例中，可能需要实施正式的成本收益分析或者评估外包或购买的方案。在这些权衡过程中，工程师和费用分析人员应该遵从 NASA 管理和预算办公室第 A-94 号通告中提供的关于备选方案比较中回报率和挣值计算指南。

3) 难以度量的费用

实际中，某些费用估算有特殊问题。这些对 NASA 系统并不独特的特殊问题通常发生在两个领域：①备选方案在尽量减少人员损失方面存在差异；②存在外部效应。如发射系统引起的污染和产生的空间碎片，即因外部效应而被迫增加费用的两个例子。因为这些费用无法用货币衡量，通常称为无法衡量的费用。在权衡分析中处理这类费用不是忽略它，而是像其他费用一样对其保持跟踪。如果这些单元是权衡空间的一部分，建议应用 A-94 号通告中的方法进行权衡。

2. 控制寿命周期费用

项目负责人/系统工程师必须保证寿命周期费用概率估算与 NASA 的预算和战略重点相协调。目前的政策是由项目提交一份预算，能够充分保证在计划资源内达到目标的概率为 70%。项目负责人和系统工程师必须确立在项目每个阶段估算、评估、监测和控制项目寿命周期费用的流程。

系统工程流程中的早期决策总是对系统寿命周期费用有最大的影响。典型地，在选定满意的系统架构时，50%~70%的系统寿命周期费用已经固定下来。到初步系统设计方案选定，确定的费用可能高到 90%。对于主持这个选择过程的系统工程师，这是其必须面临的主要难题。就在最关键的决策时刻，关于备选方案的信息最不确定。费用的不确定性是系统工程的事实，这个不确定性必须通过对项目风险进行完整和细心的分析，以及为保证项目成功预留足够的（费用、技术和进度）余地来适应。有许多估算技术可以帮助系统工程师和项目负责人处理不确定性和未知需求。关于这些技术的更多信息参见《NASA 费用估算手册》。

上述表明在项目寿命周期早期（阶段 A 和 B）更好的获取关于每个备选方案寿命周期费用信息的努力有潜在的高回报。系统工程师需要辨识主要的寿命周期费用影响因素，以及与

系统设计、制造、使用相关的风险。因此，在系统工程流程早期，引入专业工程知识如可靠性、维修性、保障性和运用工程对这样的系统是非常重要的，因为这些知识是适当估算寿命周期费用的基础。

控制寿命周期费用的机制是确立一个寿命周期费用管理计划，作为项目管理的一部分（寿命周期费用管理有时又称“准寿命周期费用设计”）。这个计划将寿命周期费用确立为设计目标，可能以采办费用或使用和保障费用作为子目标。更为具体的，寿命周期费用管理计划的目标如下：

- 确认寿命周期费用估算基本规则和假设公共集。
- 管理费用控制基线并依据后续费用变化文档保持技术控制基线的可追溯性。
- 确保采用最优方法/工具/模型进行寿命周期费用分析。
- 在项目寿命周期内，追踪所估算的寿命周期费用。
- 最重要的，通过权衡研究和正式变更请求的评估，将寿命周期费用影响因素集成到设计和开发流程中。

权衡研究和正式变更请求的评估为平衡系统的效能和寿命周期费用提供方法手段。将寿命周期费用影响因素集成到设计和开发流程的复杂性不可低估，但其可用于度量费效比的好处同样也不可低估。大量潜在的寿命周期费用权衡的存在将使得这个复杂程度加大。

3. 费用估算方法

在工程寿命周期内使用多种费用估算方法。这些方法包括参数法、类比法和（底层）工程方法。

- **参数法：**参数费用模型在项目开发的早期阶段使用，那时只有有限的工程和技术定义。该模型涉及在足够详细的聚集层采集相关历史数据，并且通过使用数学技巧生成费用估算关系将其与待估算的领域联系起来。通常这种方法相对其他方法需要较少的细节。
- **类比法：**这种方法多数情况下面向可参照已有工程或与之相近的工程，或面向由现有组件重新简单组合而来的新工程。采用进行中或者已完成的类似工程的实际费用，针对复杂性、技术或物理差异进行调整而得到新系统的费用估算。这种方法在缺少实际费用数据作为详细计算基础，但是有足够数量的工程和技术定义时使用。
- **（底层）工程法：**这种方法将工作分解结构中描述的每个组织待开展工作的费用估算自底向上累积得到估算结果。恰当实施可以令底层估算非常精确，但是每当遇到“如果——怎么样”问题，就要重新估算。任何假设变化至少使原有估算部分无效。因为得到底层估算的过程通常密集消耗时间和劳动力，在权衡研究中这种估算的可用次数是非常有限的。

费用估算方法的类型取决于工程的适当定义、要求的详细程度、数据的可用性和时间约束。例如，在工程的早期阶段，概念研究中考虑备选方案时，暂不需要实际费用数据，且将工程定义限制在待估算系统上。这时参数法模型可能是一个不错的选择。一旦设计控制基线已确定并且工程进行了更适当的定义，类比法比较适用。如果有了累积的详细实际费用数据，就可以使用工程法。关于费用估算方法和费用估算研究的更多信息可以在《NASA 费用估算手册》中找到。

4. 完整寿命周期费用估算的综合集成费用模型

许多参数费用模型可用于计算 NASA 系统成本。当前使用的典型模型可以在《NASA 费用估算手册》的附录中找到。遗憾的是,没有哪一个单独模型能充分估算各类寿命周期费用。汇总寿命周期费用常常需要结合使用这几个不同模型(某个模型伴随另外两种方法)。不管是由参数模型、类比模型或工程方法产生,硬件单元的费用估算必须经常“包装”或因因子化来估算系统的管理、系统工程、试验等相关的费用。NASA 总体费用也必须作为因子考虑。

为了集成不同模型估算的费用,系统工程师应该保证模型的输入和假设是一致的,保证模型覆盖所有寿命周期费用的相关组成,保证费用阶段的正确。来源不同且必须合并的费用估算以不同的年度定价货币表示。必须适当考虑通货膨胀因素使得总的寿命周期费用用于实际年度货币构建。关于新工程的通货膨胀率和在建工程的预算提案的通货膨胀率计算指南可以在年度 NASA 战略指导中找到。

费用模型通常根据硬件产品的首件生成费用估算,而当项目需要多件硬件时,可以应用首件产品的学习曲线获得所需的多件费用估计。学习曲线基于的概念是,随着生产的硬件总数增长,生产每个新的硬件所需要的资源则下降。学习曲线概念主要用于需要高度重复和密集劳动的不间断制造和组装任务。学习曲线的大前提是每次产品数量翻倍时,生产产品所需要的资源(工作时间)相对于前期资源需求量将减少一个确定比例。学习曲线的两种类型是单件曲线和累积平均曲线。系统工程师可以在《NASA 费用估算手册》中学习到更多关于学习曲线计算和使用的内容。

这些模型通常提供采办工作总的费用估算,而不提供寿命周期的分段费用建议。在详细项目进度表无法作为构建工作分段的基础时,系统工程师可以依据此类项目采办费用前期递增和后期递减的典型趋势,采用一组分段的算法。正态分布曲线或贝塔曲线是用来有效描述费用估算参数化散布的函数,也适合于描述产品研制合同的在初始阶段费用缓慢累积且到接近合同执行中点逐渐增加的情况。贝塔曲线是以时间为横轴以费用为纵轴在两个时间点之间的曲线。贝塔曲线的更多内容参见《NASA 费用估算手册》的附录。

尽管已经有了可用于空间系统的参数费用模型,但是还需要花费相当大的气力学习如何合理使用该模型。对于项目来说,在已有费用模型范畴之外,可能需要新的费用模型来支持权衡研究。开发新模型的工作应该在项目周期早期进行,以保证在系统工程流程中及时应用。不管是使用已有的或新建立的模型,系统工程管理计划和相关的寿命周期费用管理计划应该明确在项目寿命周期的每个阶段(如何)使用哪个模型。

6.1.2.3 经验总结

不对项目相关的经验教训进行有效的总结和集成,技术规划指导的章节就没有完成。

1. 经验总结中系统工程的作用

系统工程师是系统经验总结的主要使用者和贡献者。经验是通过实践得到的知识和理解,不论是成功的试验或使命任务,还是出现意外或失败皆如此。系统工程师为编制历史文档、需求依据和其他辅助数据分析而收集经验。系统工程专业人员收集源自工程和项目规划、关键决策点、寿命周期阶段、系统工程流程和技术评审的经验。系统工程师的责任包括通晓如何利用、管理、创建和存储经验,以及进行基于知识管理的实践。

2. 利用最佳实践的经验

经验对未来的工程、项目和流程非常重要，因为它代表来自先前项目和流程的假设和深刻理解。专业人员决定先前流程和任务的经验如何影响当前项目的风险，同时应用所总结的经验改进项目的设计和性能。

为了在项目或任务的开始吸取经验教训，需要做到如下：

- 对于新的工程或项目，使用感兴趣的关键字查询 NASA 经验总结信息系统资料库。记录经验的流程在 NPR7120.6《NASA 经验总结流程》中说明。另外，做类似工作的其他组织可能有可用的公共经验资料库。例如，化学安全委员会就有一系列事故案例研究报告。
- 各工程学科的有用经验应该在工程和项目规划中反映。即使仅发现很少信息，也要记录查找经验的过程。
- 按主题和/或学科编制经验。
- 评审和选择特殊经验中获得的知识。
- 确定得到的经验是否可能代表当前工程或项目的潜在风险。
- 将获得的知识融入项目资料库，用于风险管理、费用估算和任何其他辅助数据分析。

例如，一个正在构建空间飞行器仪器概念的系统工程师可能使用关键字“环境”、“事故”或“技术状态管理”查询经验资料库。可能查询到一个编号#1514 的经验。这个经验来自 Chandra 工程^①。该工程在 1992 年的控制基线调整移除了两个仪器，将 Chandra 从近地轨道变更为高椭圆轨道，并且简化了温度控制概念，即将原先某个被移除仪器所必需的主动温度控制简化为被动的偏冷表面辅以加热器。这个温度控制概念的变更指定采用镀银特氟纶温度控制表面。如此导致严峻的空间飞行器充电和静电释放环境。根据资料，这个事件需要极具挑战的静电释放试验和电路保护工作，花费超过一百万美元。特氟纶温度控制表面加上高椭圆轨道造成未考虑到的静电问题，说明针对一个环境的设计方案在另一个环境中并不一定适合。得到的经验是任何轨道修正应该触发一个新的从需求定义开始的完整的系统工程流程迭代过程。在做出新的设计决策之前，工程控制基线的重新确定应该考虑自然环境的变化。当正在进行的工程中控制基线发生变更时，这些经验将很有价值，应牢记在心。

3. 最佳实践经验的管理

经验的获取取决于良好的管理实践和专业知识。经验几乎经常被忽略，因为它们没有在寿命周期各阶段内及各阶段之间开发和管理。有一个趋势是等待直到问题解决后方记录经验，但是最初问题如何出现是有价值的信息，并且难以重现。当问题出现时记录下经验是非常重要的，特别是直到后续阶段才找到解决方案的时候。鉴于详细经验难以从人的记忆中恢复，等待直到技术评审或项目结束再收集经验，将阻碍经验的使用和实践的发展。在问题发生时即管理和利用经验的机制，如每月简要总结经验或定期经验分享研讨，能促进将经验融入实践及将经验带入下一个阶段。

在寿命周期每个阶段结束时，专业人员应该使用系统工程流程和技术规程化的任务作为控制门提示此项工作。为了顺利进入下一个阶段、流程或任务，必须管理所有通过控制门的信息。

系统工程工作者应该保证所有现阶段获得的经验是简明的并且是确凿的。确凿的经验包

^① Chandra 在古印度语中是“月亮”、“月光”的意思。Chandra X 射线深空望远镜在 1999 年 7 月 23 日由美国“哥伦比亚”号航天飞机送入太空。

含了一系列概要叙述和驱动事件。判断不清的经验可以放到下一阶段等待适当的支撑证据。项目负责人和项目技术团队应该确定在寿命周期所有阶段、主要系统工程流程、关键决策点和技术评审结束时所获得的经验是否记录到 NASA 资料库中。

6.2 需求管理

需求管理活动用于对所有利益相关者的期望、客户的需求、自顶向下直到最底层产品组件的技术产品需求（下文中通称为“期望与需求”）进行管理。需求管理流程的作用如下：

- 在系统设计阶段对工作分解结构模型产品定义中设定控制基线并使用的需求进行管理；
- 提供可达顶层工作分解结构模型需求的双向可追溯性；
- 在系统产品寿命周期中对所建需求控制基线的变更进行管理。

注：需求可能来自于易被忽略的利益相关者并且可能不直接支持当前的使命任务及其目标，而只是提供一个获得有益于 NASA 或国家的额外利益与信息的机会。在流程的早期，系统工程师能够帮助确定系统的潜在应用领域，收集与主要使命任务不直接相关的独特信息。通常外围组织在流程接近结束之前并不能意识到系统的目标与能力。

6.2.1 流程描述

图 6.2-1 给出了需求管理流程的典型流程图，图中给出了进行需求管理中需要考虑的典型输入、活动及输出。

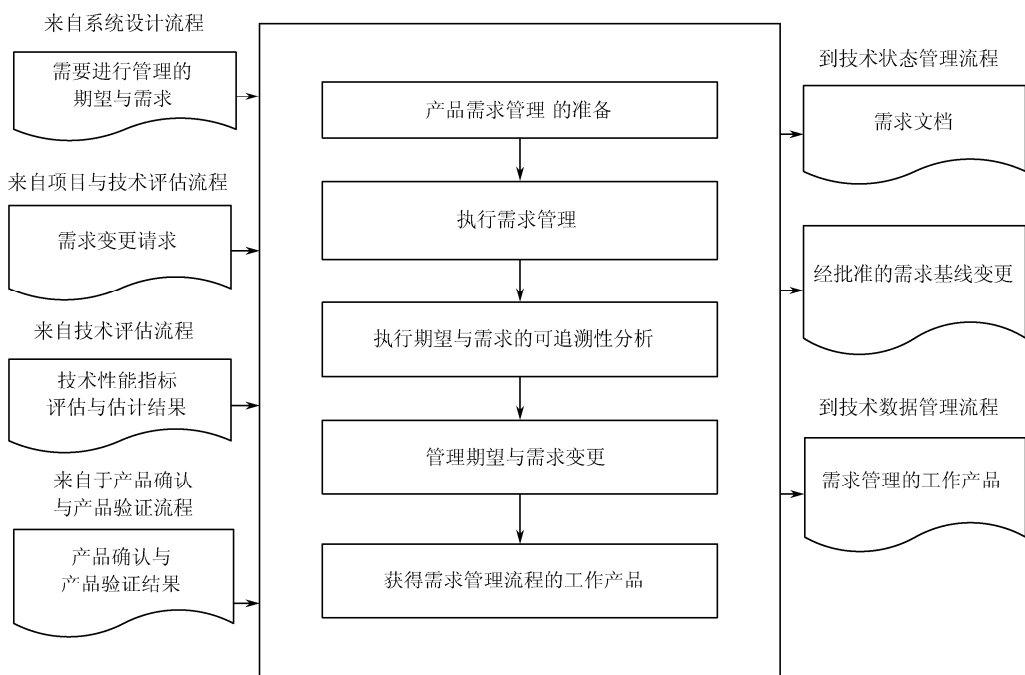


图 6.2-1 需求管理流程

6.2.1.1 输入

需求管理流程有若干基本的输入。

- 在系统设计流程中确定的需求及利益相关者的期望，该输入主要来自利益相关者期望定义流程与技术需求定义流程；
- 需求管理流程必须准备处理的需求变更请求，这种变更可能出现在项目寿命周期的任何时刻，主要来自于作为技术评估流程一部分的评审与评价结果；
- 来自技术评估流程的技术性能指标评估/评价的结果，可以就设计满足选定关键技术参数需求的适合度给出早期判断。产品性能相对于期望值的偏差可能导致需求的变更；
- 来自产品验证和产品确认流程的产品验证和确认结果，该结果直接映射到含有需求确认与验证目标的需求数据库。

6.2.1.2 流程活动

需求管理流程包括在产品的整个寿命周期中对期望与需求控制基线的变更进行管理；保持在利益相关者期望、客户需求、技术产品需求、产品组件需求、设计文档与试验计划和技术规程之间的双向可追溯性。成功的需求管理的关键活动如下：

- 建立执行需求管理的计划；
- 从系统设计流程获得需求并将它们组织成层次化树状结构；
- 在需求之间建立双向的可追溯性；
- 按照利益相关者期望、使命任务目标及约束、运行使用目标、使命任务成功准则对需求进行确认；
- 为每一个需求定义验证方法；
- 为需求设立控制基线；
- 评价项目寿命周期中需求控制基线的变更请求，实施经过变更委员会批准的变更请求；
- 维护需求、运行使用构想和架构/设计间的一致性，并着手采取消除不一致性的更正行动。

1. 需求的可追溯性

在记录每一个需求的同时，应当记录其双向可追溯性。对每一个需求，应当回溯其控制基线文档中的“高层需求/源需求”或期望，或确定其“自源性”并从更高层的需求源寻求其一致性。自源性需求可以是源自从局部角度采纳为良好实践的需求，或者是执行在逻辑分解流程与设计方案流程的活动中的设计决策结果时所产生的需求。

如果可能应对需求进行独立的评价，以确保需求追溯关系的正确性，并确保其完备表达高层需求。如果不能对需求进行独立评价，这些需求必须完全实现高层需求并放入追溯性矩阵中。此外需确保所有记录的顶层需求已经分配至较低层次的需求中。如果出现没有高层需求而又是不可接受的自源性需求，那么只能或者假设追溯流程存在缺陷而需重新进行，或假设此需求是一个“画蛇添足”的需求而应当剔除。各层之间需求冗余必须清除。如果需求是在较低层次的简单重复，且不是外部强加的约束，则该需求在较高层次可能不再是需求。需求的追溯性通常以需求矩阵的形式记录（参见附录 D）。

追溯性定义

- **追溯性**：在两个或者更多的逻辑实体诸如需求、系统单元、验证或者任务之间的可辨识的联系。
- **双向追溯性**：在两个或者更多的逻辑实体之间双向的可辨识联系(如指向或者发自实体)。

2. 需求确认

需求管理的一项重要工作是根据利益相关者的期望、使命任务目标与约束、运行使用目标及任务成功准则进行需求确认。需求的确认主要包括如下三个步骤。

(1) **需求是否正确书写**：确认并更正以“需要”形式陈述需求时的格式错误和编辑错误；

(2) **需求在技术层面上是否正确**：在将需求交给利益相关者评审之前，技术团队中训练有素的评审人员要辨识并尽可能多地去除技术错误。

评审人员应当对需求陈述做如下检查：

- 需求对于控制基线设定的利益相关者期望是否具有双向可追溯性；
- 所用的假设是否合理；
- 需求对产品方案的设计和实现满足产品寿命周期中生产阶段成功准则是否重要并与其一致。

• **需求是否令利益相关者满意**：所有相关的利益相关者团体检查并去除需求缺陷。

需求确认的结果常常是决定项目能否进入逻辑分解或设计方案定义下一流程的关键因素。项目团队应该做好以下准备工作：

- 证明项目需求是完备的和可理解的；
- 证明有序的评价标准与需求是一致的，并且与使用和保障概念是一致的；
- 确认需求和评价标准与利益相关者的需求一致；
- 证明运行使用构想及架构概念可以支撑使命任务需要、目的、目标、前提、方针和约束；
- 证明管理需求变更的流程已经在项目的知识库中建立和记录，并已经与利益相关者交流。

3. 管理需求变更

在项目的阶段 A 与阶段 B，可能会发生需求和约束的变更。对变更进行充分的评估十分重要，以确定其对架构、设计、接口、运行使用构想及高层和低层需求的影响。进行功能分析和敏感性分析可以确保需求切合实际并均匀分配。严苛的需求验证与确认过程确保需求能够满足并且符合使命任务目标。所有需求变更必须遵从评审和审批环节，以维持可追溯性并确保其对系统所有部件的影响被完全评估。

一旦完成需求确认并经过系统需求评审流程，需求即被置于正式技术状态控制之下。这样，任何需求变更都必须经过技术状态控制部门的批准。系统工程师、项目负责人及其他关键工程师通常参与技术状态控制部门的审批流程，评估需求变更对成本、性能、流程及安全性方面的影响。

技术团队还应该确保及时地与相关人员交流经批准的需求。每一个项目都应该建立追踪和传递最新项目信息的机制。关于技术状态管理更详细的信息可以参见 6.5 节。

4. 需求管理的关键问题

1) 需求变更

需求变更的有效管理需要在变更被批准与实施之前，对提议的变更进行影响评估。通常，这通过应用技术状态管理流程来实现。为了使技术状态管理具有此功能，必须归档控制基线技术状态，并归档评估变更对控制基线影响的工具。用于分析变更带来影响的典型工具如下所述。

- **性能余量列表：**这个工具是系统关键性能余量及其当前余量状态的列表。例如，推进剂性能余量将参照完成任务所必需的推进剂量提供必要的可用的推进剂余量。必须评估变更对性能余量的影响。
- **技术状态管理主题评估人员名单：**这份名单由项目管理办公室开发，目的是确保由合适的人员评估变更和变更的影响。所有变更需按顺序送到合适的人员手中，确保辨识出变更的所有影响。这份名单需要定时更新。
- **风险分析系统与威胁列表：**风险分析系统可以用来辨识项目的风险及风险与成本、进度、技术方面的关联。控制基线的变更可能影响辨识风险的结果和似然性，或给项目带来新的风险。威胁列表通常用来辨识与项目所有风险相关的费用。项目储备用来减低相关风险。分析对比威胁列表确定的需求及可用储备，有助于确定储备使用优先序。

管理需求变更的流程需要考虑与变更过程中制定决策相关的信息发布。技术状态管理流程需要就需求变更的决策与对决策有影响的组织沟通。在审批变更的相关委员会会议上，更新归档文件的行动应该作为一部分包含在全套变更之中。应该对这些行动进行追踪，以确保对决策有影响的文档能够及时更新。

2) 反馈到需求控制基线

在系统组件的开发过程中，需要不断向需求提供反馈。这种反馈通常在产品的设计、确认及验证流程中产生。向项目的反馈包括影响系统的接口及运行使用的设计实施问题。在许多情况下，产品的设计可能会对于组件如何运行、维护及存储带来一些约束。这种信息需要与项目团队交流，以便评估其对系统运行使用或架构设计的影响。每个系统组件都对自身的设计和运行使用做优化。而系统工程师的作用就是评估这种组件级的自身优化对整个系统优化带来的影响。

3) 需求渐增

“需求渐增”是用于描述项目实施过程中需求细微增加变化的术语。在开发过程中需求集合的尺度呈现出持续增长的趋势，这种趋势导致系统比原先预期的更加昂贵和更加复杂。通常来说，这种变化并不是有意为之，并且表面来看，这些变化似乎的确使系统性能得到提升。

然而，在技术需求定义流程中某些需求的渐增可能包含实际上并不存在的新需求，事先无法做出预测。这些新的需求是演化的结果，并且在构建系统的过程中，这些需求不能忽略。避免或者尽量减少需求渐增现象的几项技术如下：

- 在需求定义阶段的早期，列出可能已经注意而未被陈述的、未察觉的，甚至难以想象的需求。
- 建立严格的需求变更评估流程，作为技术状态管理流程的一部分。
- 为递交变更申请设立官方渠道。这将明确谁有权生成变更请求并将其正式提交技术状态控制部门（例如，合同指定的代表、项目技术负责人、客户/研究团队领导、用户等）。
- 度量每个需求变更请求的功能性并评估变更对系统其他部分的影响。比较这些影响与变更未被批准后果的差异。如果不批准变更会有什么风险？

- 确定变更提议能否在财务及技术资源预算内被容纳。如果在资源余量内不能满足变更的需求，则变更就很有可能被拒绝。

6.2.1.3 输出

需求管理活动的典型输出如下所述。

- **需求文档：**在确定需求控制基线时，需求文档将提交至技术状态管理流程。这些文档的官方控制版本通常在项目选定的需求管理工具中以电子文档格式保存和维护。以这种方式，需求文档可关联到包含其所有可追溯关系的需求矩阵中。
- **经批准的需求控制基线变更：**这些需求控制基线变更是在仔细评估需求变更对整个产品或整个系统可能带来的所有影响之后，作为技术状态管理流程的输出发布的。即使是单个变更也可能会产生深远的连锁影响，从而可能导致大量文档中的某些需求变更。
- **多种需求管理工作产品：**需求管理工作产品包括所有的报告、记录，以及那些不需提交的需求管理流程的结果。例如，作为应用在验证与确认报告中工作产品的双向可追溯性的状况。

6.2.2 需求管理指南

6.2.2.1 需求管理计划

技术团队应该为执行需求管理活动准备好计划。该计划通常是系统工程管理计划的一部分但又相对独立。需求管理计划应该做到如下：

- 确定需求管理流程的利益相关者（如那些可能影响产品及流程或被产品及流程影响者）。
- 为执行需求管理技术规程与活动提供进度表。
- 为执行需求管理活动分配责任、进行授权，以及安排适当的资源，开发需求管理的工作产品，并提供在需求管理活动中定义的需求管理服务（如工作人员、需求管理数据库工具等）。
- 为所有的需求管理工作产品定义其技术状态管理/数据管理的级别。
- 确定需要对执行需求管理活动的人员进行的培训。

6.2.2.2 需求管理工具

对于小型的项目或产品而言，可以用电子表格程序进行需求管理。但是较大的工程和项目需要使用有效的需求管理工具。在进行需求管理工具选择的时候，为了确定在需求管理数据库工具中需求如何组织及工具如何使用，定义项目的技术规程是重要的。依据现代需求管理工具，创建一个需求管理数据库，根据技术团队的特定需要以多种方式对需求数据进行分类和存储是完全可能的。数据库的组织并不是一件琐碎的工作，其重要意义在于项目寿命周期中如何看待需求数据。组织数据库可以获得技术团队可能需要的所有视角的需求信息。应当仔细考虑需求和双向可追溯性的分解如何在数据库中描述。成熟的需求管理数据库工具同样有获取需求矩阵中大量需求属性的能力，如需求可追溯性和需求分配关系。对于在需求矩阵中的每一个需求而言，进行验证的方法、层级、阶段等信息将被记录在需求管理数据库工具（如与每个需求的方法、层级、阶段等属性相关的工具）中的验证需求矩阵中。另外，确保需求管理数据库工具与为项目所选择的验证和确认工具之间的兼容性也是非常重要的。

6.3 接口管理

接口管理与控制对于工程或项目的成功至关重要。接口管理是在不同团体（如政府部门、承包商、不同地域分布的技术团队等）中分解工作时辅助控制产品开发的过程，也是定义和维护需要互操作的产品之间一致性的过程。

6.3.1 流程描述

图 6.3-1 描述了接口管理流程的典型流程图，图中给出了接口管理需要考虑的典型输入、输出及活动。

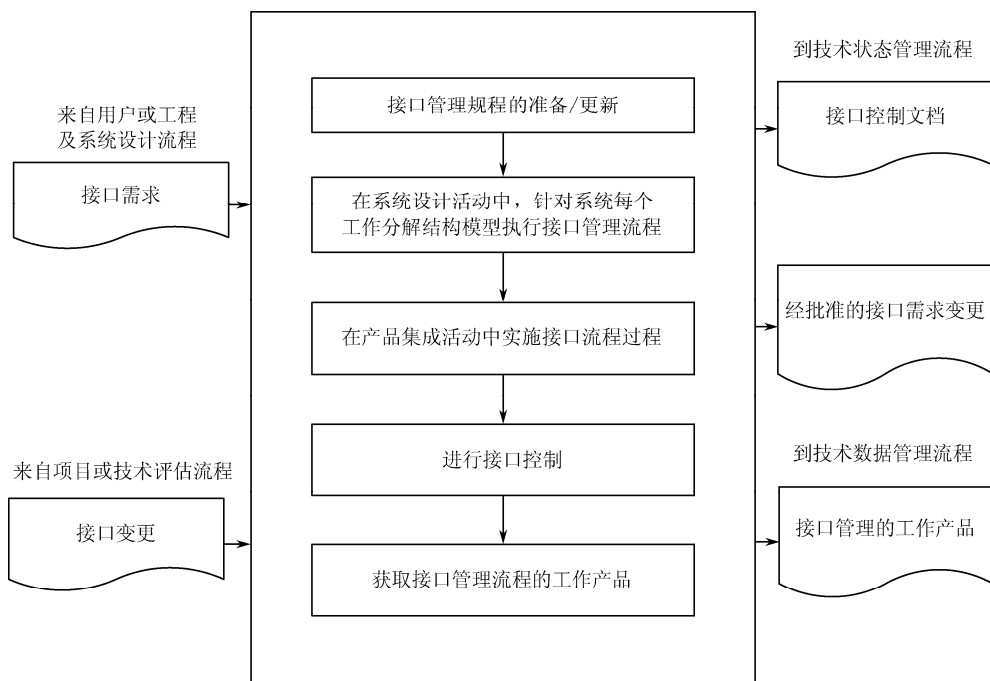


图 6.3-1 接口管理流程

6.3.1.1 输入

理解和进行接口管理需要考虑的典型输入如下所述。

- **系统描述：**系统描述支持对系统设计的探索与检查，以确定系统接口存在的位置。对承包商的安排也同样需要指定接口之处。
- **系统边界：**系统边界记录系统的物理边界、系统的组件和/或子系统，这也是确定接口存在位置的导向。
- **组织结构：**组织结构决定哪个组织规定接口，特别是当需要在系统共享接口参数方面达成一致时，工程和项目的工作分解结构也提供接口边界。
- **部门结构：**系统工程管理流程（系统工程管理计划）有助于确定组织接口职责并明确接口的位置。

- **接口需求：**内部和外部的功能接口需求及物理接口需求将作为产品技术需求定义流程的一部分被开发。
- **接口变更请求：**这些变更包括产生于工程或项目协议的变更，或作为技术评估流程的一部分来自技术团队部分的变更。

6.3.1.2 流程活动

在项目规划论证阶段，分析产品的运行使用构想以确定内部和外部接口。这项分析将建立起需要记录和维护的接口起点、终点、激发及其他特性。随着系统结构与架构的显现，需要加入新的接口，而已有接口则可能需要更改且必须维护。因此，接口管理流程与其他领域有很紧密的关系，例如，此阶段中的需求定义流程与技术状态管理流程。通常接口工作小组建立通信链接负责在系统、目标产品、辅助产品与子系统之间的交互。接口工作小组的责任是确保完成所有接口活动的计划、进度安排和执行。显然接口工作小组是一个技术团队，由来自各个接口相关团体（如项目管理部门、承包商等）的适当技术成员组成。

在产品集成流程中，接口管理活动支持对集成与组装技术规程的评审，以确保接口被正确地标记并与相关规范及接口控制文件相一致。接口管理流程与验证确认流程存在着紧密的关系。接口控制文档与经批准的接口需求变更被用做产品验证流程与产品确认流程的输入，尤其是在需要用验证试验约束和接口参数来设定试验目标与试验计划时。接口需求验证是整个系统验证的一个关键方面。

6.3.1.3 输出

进行接口管理需要获取的典型输出包括接口控制相关文档。此类文档确定并获得接口信息和经批准的接口变更请求。接口文档的类型包括接口需求文档、接口控制文档/接口控制图、接口定义文档，以及接口控制计划。这些输出将通过运用技术状态管理流程来维护和审批，并将成为整个项目技术数据资料的一部分。

6.3.2 接口管理指南

6.3.2.1 接口需求文档

接口需求定义了存在于两个或多个系统、系统功能、系统单元、状态控制项等之间系统公共边界上的功能的、性能的、电子的、环境的、人因的、物理的需求与约束。接口需求包括逻辑接口需求与物理接口需求。按照需要划分，接口通常包括物理度量、能量或信息传输序列的定义，以及所有其他重要的交互关系。例如，通信接口包含系统内部，以及系统与其环境之间数据和信息的流动与传输。通信需求的适当评估牵涉到通信的结构元素（如带宽、数据率、分布等）与内容性元素（如用于通信的数据/信息、系统组件之间流动的数据/信息、这些数据/信息对系统功能性的重要度）的定义。如果功能输入与输出已经定义，接口需求可以从功能分配中衍生出来，例如，

如果功能 F1 的输出内容 A 作为功能 F2 的输入，且功能 F1 由组件 C1 来完成，且功能 F2 由组件 C2 来完成，则表明在组件 C1 与组件 C2 之间的接口传输内容为 A，不论内容 A 是固态、液态还是包含数据的消息。

接口需求文档定义两个或多个系统产品、单元、组件之间所有物理的、功能的、流程的

接口需求,并确保项目硬件、软件之间的兼容性。接口需求文档由物理的和功能的需求和约束、硬件状态控制项与软件状态控制项组成。接口需求文档的目的是控制开发中的系统内部相互关联的组件之间接口,控制开发中的系统与属于同一整体架构的其他(已存在或开发中)外部系统之间的接口。具体的接口需求可能包含在系统需求文档中,直到开发过程中完成对每个单个接口的定义。当各个组织分别开发系统组件时或当系统必须从工程/项目控制之外的其他系统获取需求时,接口需求文档是非常有用的。在阶段 A 和阶段 B,可以为接口的不同层次草拟多个接口需求文档。应用系统需求评审完善系统到外部系统的接口(如航天飞机与国际空间站之间)和部件到部件的接口(如航天飞机与发射台之间)。关于接口需求文档的一般性概述参见附录 L。

6.3.2.2 接口控制文档或接口控制图

接口控制文档或接口控制图详细刻画系统单元之间的物理接口,包括连接的数目和类型、电子参数、机械性质及环境约束。接口控制文档明确接口需求的设计方案。当不同的组织分别开发某个设计方案的特定接口时,接口控制文档的作用就会显现出来。

6.3.2.3 接口定义文档

接口定义文档是由目标产品提供者单边控制的文档,主要为已建立的设计方案提供接口细节。该文档有时被称为“单向接口控制文档”。接口定义文档为其用户提供已有设计中连接件、电子参数、机械性质、环境约束等方面的说明。接口用户必须兼容已有的设计接口来设计系统的接口。

6.3.2.4 接口控制计划

接口控制计划应当按照已确定的接口控制流程来开发,并与接口文档关联。接口控制计划的关键内容就是给出接口的分类列表并指出每个接口的拥有者。接口控制计划还应考虑技术状态控制问题及文档变更流程的实施机制(如初步接口修订通告/接口修订通告)。

典型接口管理清单

- 使用接口需求文档开发时提供的一般性概述,为当前不可用的段落或小节定义一个“保留”位置。
- 确保有两个或者更多的规范用来作为接口需求文档中特定需求的父本。
- 确保使用“需要”形式的陈述来定义特定需求。
- 接口需求文档必须被所有相关的组织批准和签署。
- 必须建立管理接口需求文档变更的控制流程。
- 基于接口需求文档中的需求开发相应的接口控制文档。
- 确认接口需求与产品验证流程及产品确认流程之间的连通性。
- 定义表述接口管理的系统工程管理流程(系统工程管理计划)内容。
- 每一个主工程或主项目应该包含接口控制计划,用于描述接口管理产品的内容和实施。

6.4 技术风险管理

技术风险管理流程是交叉关联的技术管理流程之一。风险定义为以下部分的组合:(1)一个工程或项目可能经历非期望事件的概率;(2)如果非期望事件真的发生,其后果、影响

和严重性。这个非期望事件可能是技术性或工程性原因引起的（如成本超支、进度延迟、安全事故、卫生问题、恶意活动、环境影响或未能达到所需的科学技术目标或成功准则）。概率和后果两者可能与不确定性有联系。技术风险管理是一个有组织的、基于系统风险信息决策科学，它主动辨识、分析、计划、跟踪、控制、交流、记录和管理为达到项目目的可能增长的风险。技术风险管理流程关注项目目标，作为风险管理决策和确保管理活动的分析基础，同时关注处理不确定性的框架。

风险管理的策略包括转移性能风险、排除风险、降低非期望事件发生的可能性、缩减风险的负面影响（如减小后果的严重性）、适当减少不确定性、承担部分或者全部特定风险的后果。一旦选定策略，技术风险管理流程确保其在风险跟踪和控制活动计划和实施过程中的成功执行。技术风险管理关注与技术性能相关的风险。当然，技术风险的管理通过影响预算、进度和其他利益相关者期望，对非技术风险产生影响。技术风险管理的讨论适用于技术和非技术风险问题，而本节的焦点是技术风险问题。

技术风险管理中的关键概念

- **风险**：风险是在确定的费用、进度和技术约束下对无法达到工程总体目标的能力缺乏的度量，包括两部分，即未能取得特定结果的概率，以及未能取得特定结果的后果/影响。
- **费用风险**：这是与工程或项目达到其寿命周期成本目标和获得适当资金的能力有关的风险。对费用产生影响的风险领域有两个，一个是成本估算和目标不精确不合理的风险；另一个是控制成本、进度和性能过程失败而导致的工程实施执行未能与目标成本吻合的风险。
- **进度风险**：进度风险是那些与系统开发、生产、实施和使用的时间估算和时间分配适当性相关的风险。对进度产生影响的风险领域有两个，一个是进度估算和目标不现实不合理的风险；另一个是控制成本、进度和性能过程失败而导致的工程执行未能达到进度目标的风险。
- **技术风险**：技术风险与设计的进展过程和所关心的系统生产对设计能否满足利益相关者期望的影响和对技术需求所要求的性能水平的影响相关。技术风险受设计、试验和生产流程影响（流程风险），产品分解结构中各层所描述的产品性质也受其影响（产品风险）。
- **工程性风险**：工程性风险与来自项目外部的有利行动和不利行动有关，这些行动对项目负责人来说无法控制，但可能对项目产生显著的影响。这些影响通过技术、费用和/或进度显现。这些行动包括国际武器交易规章（ITAR）、进出口控制、与国内外其他组织的伙伴协议、国会指导方针或拨款、管理和预算办公室方针、工业承包商重组、外部组织更迭等。
- **危险与风险**：危险和风险是有区别的。危险表示一种危害的潜在可能，风险不仅考虑危害的潜在可能，还包括引起不利结果的状况和可能性。在安全的背景下，“风险”考虑非期望事件后果发生的可能性。
- **概率风险评估**：概率风险评估是一个基于想定的风险评价技术，该技术量化多种可能的非期望事件想定及其后果的可能性，以及可能性和后果中的不确定性。传统上，设计组织依赖于替代标准，如系统冗余或系统级可靠性指标，部分因为直接量化实际安全性有不可逾越的困难，而找到替代标准相对简单。依靠指定目标层次的详细构建，概率风险评估可以用于量化技术性能指标，它与基本目标（如人员伤亡概率）密切相关。概率风险评估关注综合想定的开发，它直接应用于识别关键风险和可能的诱因。在所有最简单的系统中，这要求利用模型来获取重要想定、评估后果、系统地量化想定的可能性。这些模型包括可靠性模型、系统安全模型、仿真模型、性能模型和逻辑模型。

6.4.1 流程描述

图 6.4-1 描述一个典型的技术风险管理流程图，并给出进行技术风险管理需要考虑的典型输入、活动和输出。

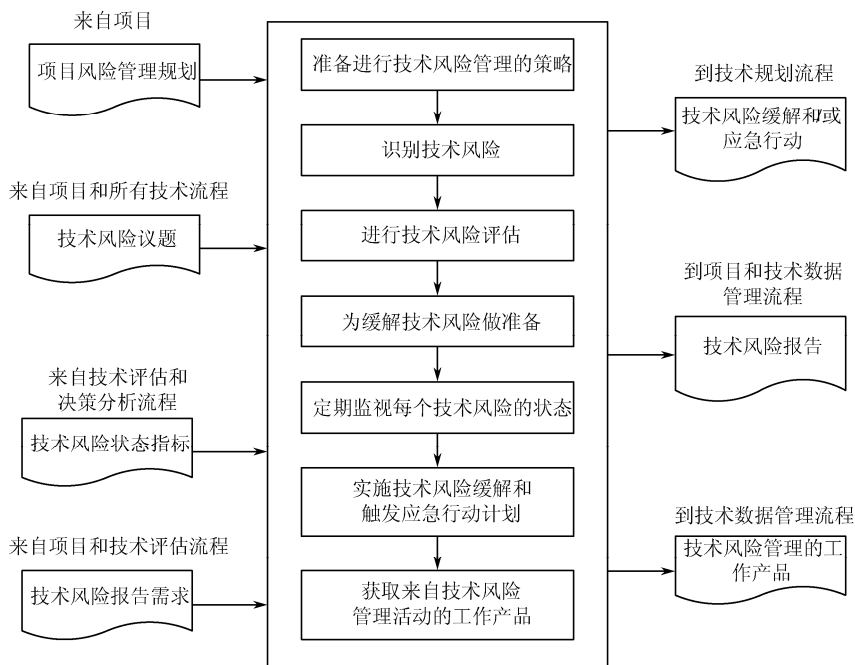


图 6.4-1 技术风险管理流程

6.4.1.1 输入

技术风险管理的典型输入如下所述。

- **计划和策略：**风险管理计划、风险报告需求、系统工程管理计划、技术数据产品形式和政策输入的指标和阈值。
- **技术输入：**技术性能指标、待评估的工程备选方案、技术议题和当前的工程控制基线。
- **备选方案风险分析需要的输入：**设计信息和相关经验数据。

6.4.1.2 流程活动

技术风险管理是一个考虑活动需求、约束和优先权的迭代过程：

- 识别并评估实施技术备选方案的相关风险；
- 分析、排序、计划、跟踪与控制风险和选定备选方案的实施；
- 需要时启动应急行动计划；
- 交流、评议、归档工作产品和已识别的风险；
- 在全寿命周期中根据新信息重复上述步骤。

6.4.1.3 输出

技术风险管理活动中的关键输出如下所述。

- **计划和策略：**依据控制基线的风险跟踪和控制计划；
- **技术输出：**技术风险缓解，应急行动和跟踪结果，状况调查和紧急事件；
- **备选方案风险分析输出：**已识别、分析、优先排序并分配的风险，风险分析更新。

6.4.2 技术风险管理指南

广泛应用的风险概念包括想定、似然性和后果等，如图 6.4-2 和图 6.4-3 所示。

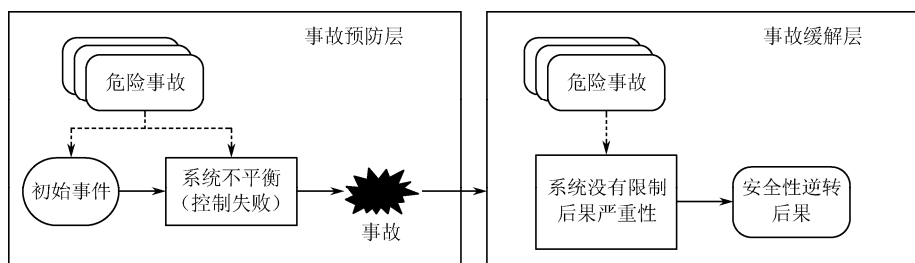


图 6.4-2 基于想定的危险性建模

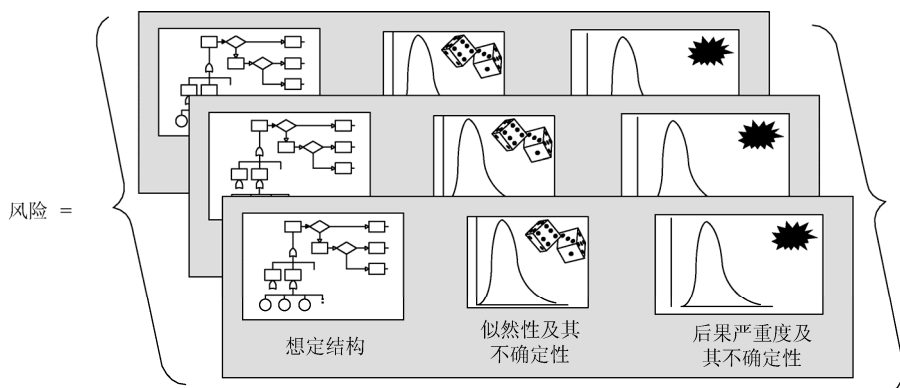


图 6.4-3 组成风险的三元组

这里的想定、后果、似然性及相关不确定性，构成完整的风险三元组（风险是想定、似然性和后果的三元组集合）。三元组概念原则上对所有风险类型适用，包括量化简化指标如期望后果所需的信息。单独估计预期后果（后果相乘得到的频率或概率）并不能充分辅助进行技术决策。基于想定的分析提供了更多基于风险信息决策所需的信息。例如，很少出现但严重的风险因素所引起的响应可能不同于常见而不严重的风险因素的响应，即使两者导致相同的预期后果。在所有最简单的系统里，需要用详细模型获取重要想定、评估后果并系统地量化想定的似然性。关于概率风险评估的更多信息参见 NPR 8705.3《NASA 管理者和专业人员概率风险评估技术规程指南》。

6.4.2.1 技术风险管理中持续风险管理的作用

持续风险管理是 NASA 内部广泛应用的技术，自始至终贯穿工程寿命周期，监测和控制风险。它是一个自适应的迭代过程，能促进对风险的成功控制。该模式中每一步建立在前一步基础上，从而通过生成信息的反馈改善设计和流程。图 6.4-4 反映持续风险管理的自适应特征。

如下是持续风险管理的一个简单综述，供参考。

- **识别：**通过识别有相反后果（偏离工程意图）的想定来识别工程的风险。持续风险管理涉及与安全、技术性能、费用、进度及其他工程特定风险有关系的风险。

- **分析：**通过分析评估风险的似然性和后果，包括似然性和后果的不确定性，以及必须采取的缓解风险行动的时间框架。
- **计划：**计划跟踪和控制行动。决定待跟踪的对象，决定正确行动的决策阈值，以及提议风险控制行动。
- **追踪：**追踪与技术性能指标有关的工程观测量（性能数据、进度差异等），度量工程性能与其计划相比的相近程度。
- **控制：**对确定的紧急风险事件，执行相应的控制行动并验证其有效性。
- **交流、评议和归档：**这是前面各个步骤都具有的元素。它遍历每个工程阶段，聚焦于理解和交流所有风险信息；归档风险、风险控制计划及结束/验收的依据；通过持续风险管理流程做出慎重决策。

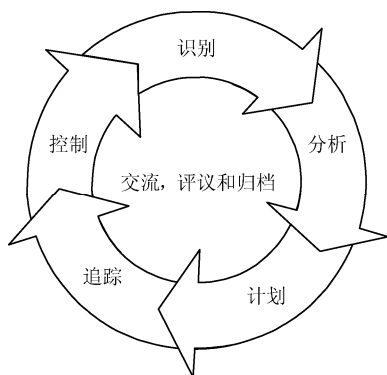


图 6.4-4 持续风险管理

6.4.2.2 持续风险管理和基于风险信息决策分析之间的接口

图 6.4-5 给出持续风险管理和基于风险信息决策分析之间的接口（关于决策分析流程参见 6.8.2 节）。源于风险的决策分析流程的步骤如下：

- 明确阐述目标层次和技术性能指标。
- 提议并明确决策备选方案。该流程的备选方案与其他系统工程流程（包括设计方案流程、验证流程、确认流程和生产流程）中确定的备选方案相结合。
- 进行风险分析并对备选方案排序。
- 评价并推荐备选方案。
- 追踪决策的执行情况。

上述步骤通过首先关注目标，其次关注根据了然于胸的目标开发决策备选方案，并运用在其他系统工程流程中开发的备选方案，支持做出良好决策。决策分析的后面几个步骤与技术风险管理流程密切相关，如图 6.4-5 所示。

决策备选方案风险分析（第三个框）不仅引导选择偏好的备选方案，还实现了持续风险管理中“识别”和“分析”两步。偏好的备选方案选择部分基于对备选方案相关风险的理解。备选方案选择之后是一个计划活动，其实施的关键已经说明，也就是风险追踪和控制，如果必要还包括风险缓解。图 6.4-5 中还概念化描述了风险管理与其他技术流程和工程流程之间的接口。

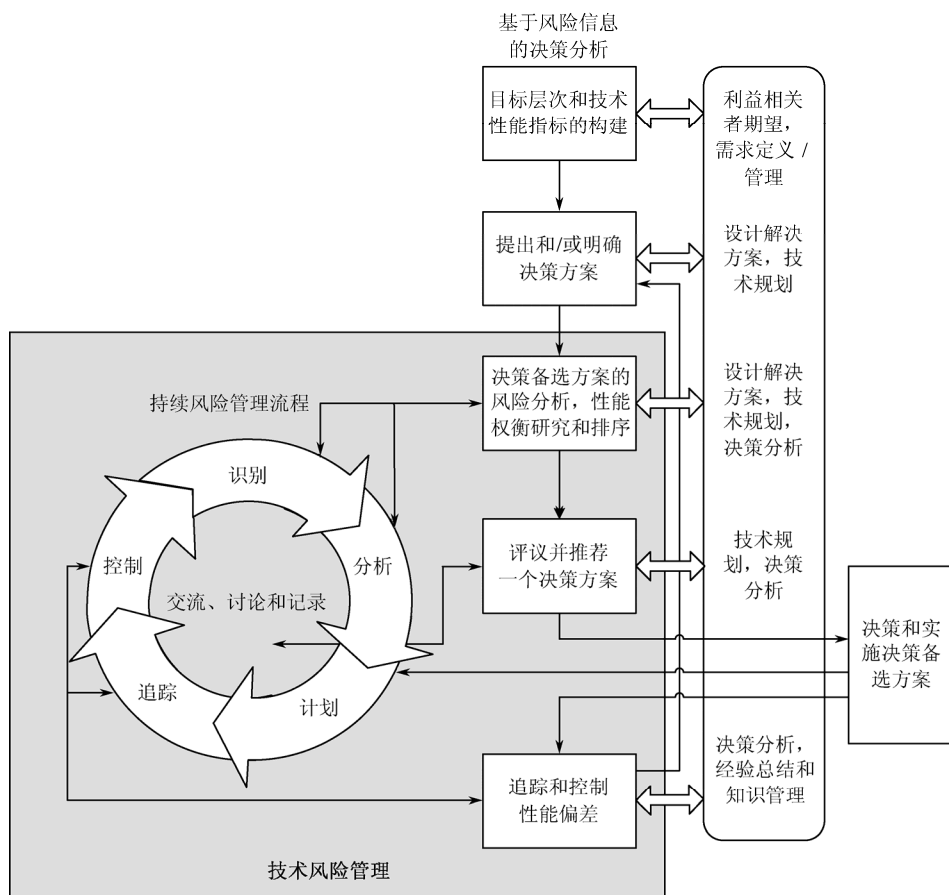


图 6.4-5 持续风险管理与基于风险信息决策分析之间的接口

风险分析、权衡研究和定级

这个步骤的目的是落实分析的种类和数量，满足风险特征化的两个目的：风险备选方案排序，执行持续风险管理中的“识别”和“分析”步骤。

为了支持排序，可能需要进行权衡研究。影响决策结果的技术性能指标被量化，包括相应的不确定性。

为了支持持续风险管理中的“识别”和“分析”步骤，与偏好备选方案相关的风险被详细分析，如图 6.4-6 所示。

风险分析可采用多种形式，范围从定性风险识别（基本想定和后果，无需使用如故障模式与影响分析和故障树等专用技术进行似然性的详细定量分析），到高度量化的方法如概率风险评估。技术状况确定后，分析即可停止；如果更简单更定性的方法足够，则不需应用更详细的方法。此时流程完成识别和计划，并被持续检查。适当方法的选择和应用在后文中讨论。

6.4.2.3 风险管理相应方法的选取和应用

问题的性质和背景及特定的技术性能指标决定需要使用的方法。在一些项目中，定性方法适合进行决策，而在其他项目中，这些方法对正确描绘问题的重要特征和分配有限的风险

缩减资源显得不够精确。技术团队需要决定风险识别和基于判断的风险特征化是否充分，或者通过更详细的风险分析得到的技术性能指标量化改进是否合理。在做出决定时，技术团队必须平衡风险分析的成本与获得更多信息的价值。“信息价值”的概念是做出“什么分析是正确的”和“什么程度的不确定性需要量化”决定的中心。

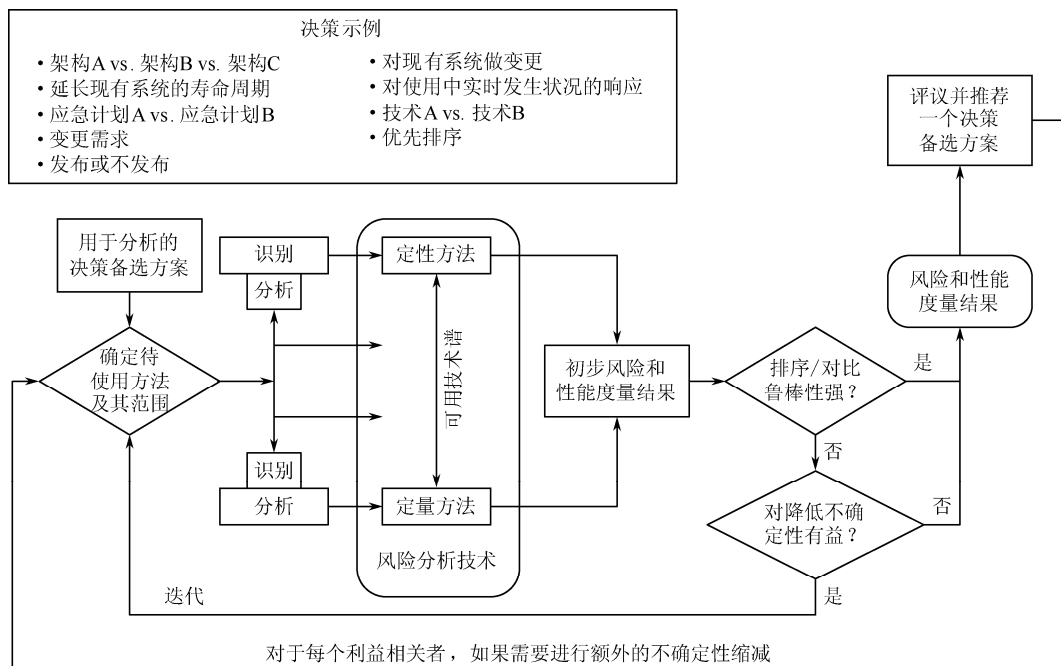


图 6.4-6 决策备选方案的风险分析

回顾先前类似项目的文档、数据和报告中的经验教训，能够为新项目的危险识别提供深刻理解和信息。这包括对相似系统和历史文件如事故文档和几近失败任务报告的研究。应用这种技术的关键在于识别先前项目和当前项目在哪些方面是相似的，先前项目的哪些数据与当前项目相关。在某些情况下，量化方法的应用可以补偿信息有限的实用性，因为这些技术在可用信息中提取最大价值。

1. 风险的种类

进行风险分类是选择正确风险分析方法的重要前提。大体上，风险与成本、进度和技术性能有关。还有许多其他类别，像安全性、组织性、管理、采购、保障性、政治因素和工程风险，而这些可以认为是广泛分类的子集。例如，工程风险表示影响成本/进度的风险，而非技术风险。

在风险分析的早期阶段，通常需要筛选风险因素以确保更详细分析的导向。基于此目的，传统的定界方法可能是合适的。风险程度的过高估计可在进行更详细分析时得到修正。但是，这可能会产生误导，用定界估计去引导风险定级。正因如此，对问题的分析需要反复迭代，从筛选估计开始，依此对后续分析优先排序，并形成更合理的基于详细分析重要因素的风险档案。这就是图 6.4-6 中反复迭代循环的部分。

风险源示例

在“识别”活动中，如下清单可作为相关领域分析人员的提示，这些领域中曾经识别出风险。

- 不切实际的进度估计或者进度安排；
- 不切实际的成本估计或预算分配；
- 不合适的人员配备或是技能配备；
- 不确定或不充足的承包商能力；
- 不确定或不充足的供货商能力；
- 不充分的生产能力；
- 运行使用方面的危险；
- 给工程技术工作造成负面影响的问题、隐患和弱点；
- 未经过评估且未经历过的工作；
- 定义不当的需求；
- 无双向可追溯性的需求；
- 不可行的设计；
- 不合适的技术状态管理；
- 难以获得的技术；
- 不充足的测试计划；
- 不充足的质量保证；
- 需求中规定产品树中过低层次的非开发产品；
- 缺乏同步开发用于部署、训练、生产、使用、保障或处置的辅助产品。

2. 定性方法

通常用定性方法完成的工作如下：

- 帮助确定存在潜在风险因素的想定；
- 为更加定量的方法提供部分输入；
- 支持基于判断的技术性能指标量化。

这些定性方法简要的讨论如下所述。

1) 风险矩阵

“ $N \times M$ ”（大部分是 5×5 ）风险矩阵为风险管理和交流提供辅助（见图 6.4-7）该矩阵兼具似然性、后果的定性和半定量度量方法。风险矩阵不是评估工具，但是可以方便风险讨论。

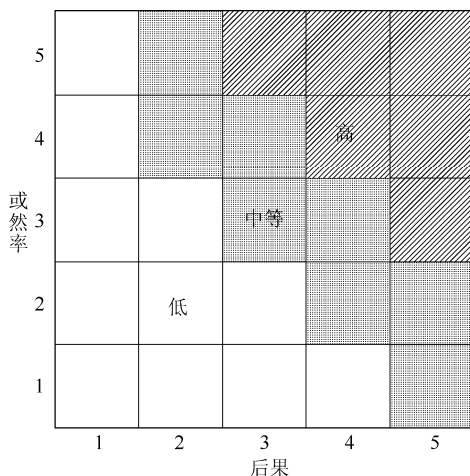


图 6.4-7 风险矩阵

明确地说，风险矩阵有助于如下情况：

- 追踪风险控制工作的情况和影响；
- 交流风险状况信息。

划分风险等级时，使用通用方法很重要。如果不同的组织或不同的项目都建立自身的格式标准，这可能引起困惑和误解。因此，在使用定级系统之前，应该通过图例或其他方式清晰地建立定义并进行交流。考虑到本手册的目的，这里给出 NASA、其他政府组织和工业部门广泛应用的定义。

- **低风险（白色）**：很少有或没有潜在的费用增长、进度中断或性能降级。工程计划范围内的行动和正常管理工作只会引起可控可接受的风险。
- **中等风险（点状）**：可能引起某些费用增长、进度中断和性能降级。控制风险可能需要特殊行动和管理工作。
- **高风险（斜线）**：很可能导致影响很大的费用增加、进度中断或性能降级。为控制风险需要采取重要的附加行动和高度优先的管理工作。

风险矩阵的局限性

- 没有考虑风险间的相互作用。每个风险单独映射到矩阵（这些风险与使用失效模式影响和危害性分析或故障树时的每一项使用相关）。
- 没有办法处理聚集的风险（即总风险）。
- 没有办法表示不确定性。考虑一个风险在给定的或然率范围和后果范围内存在，两者都需假设为已知。
- 在或然率和后果之间固化权衡。利用标准的 5×5 矩阵，或然率和后果偏差的显著水平就固定了，对工程环境不敏感。

2) FMEA, FMECA 和故障树

失效模式影响分析（FMEA），失效模式影响与危害性分析（FMECA）和故障树是用来识别产品或流程的潜在失效模式，评估这些失效模式所带来的风险，进行重要性排序，并确定和实施纠正措施，最终解决最关键问题的方法。这些方法关注构成系统的硬件组件，以及制成系统的流程。根据 MIL-STD-1629《失效模式及影响分析》，FMECA 是分析系统中每一个潜在故障的持续过程，以确定其对系统造成的后果和影响，并根据其后果的严重性区分每个潜在的失效模式。故障树用来评价导致所关心的顶事件的故障组合（见图 6.4-8）。

3. 定量方法和交流方法

概率风险评估是一个综合的、结构化的逻辑分析方法，用来识别和评估复杂技术系统的风险，以更经济高效地改善其安全性和性能。

风险管理包括防止不利的（可造成不良后果的）想定（减少其发生频率）并促进有利的想定。这需要了解不利想定的因素方能防止其发生，需要了解成功想定的因素方能对其进行促进。

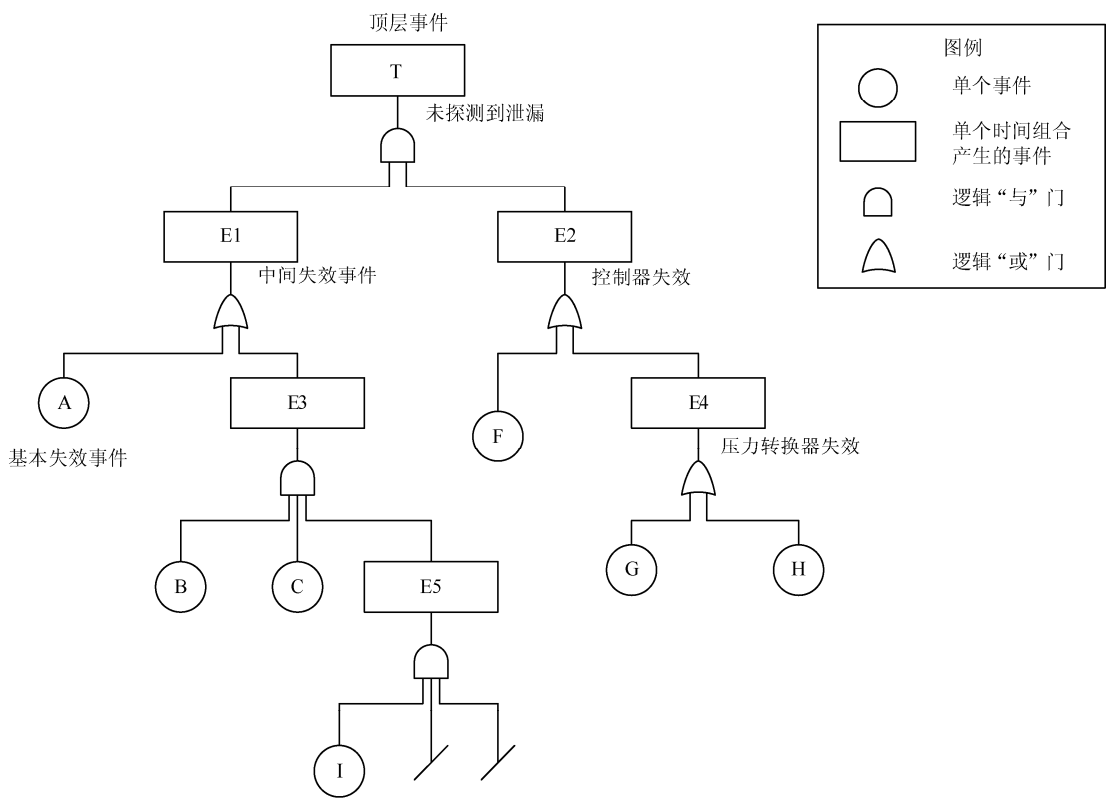


图 6.4-8 故障树示例

概率风险评估量化风险指标。风险指标是指一类可能会出现在决策模型中的度量值。例如，特定等级后果或预期后果发生的概率或频率。NASA 关心的风险指标包括某些特定使命任务类型中损失飞行器的概率、使命任务失败的概率，以及损失大量资金的概率。类似系统故障概率的品质因素可以用做风险指标，但是风险指标通常意味着更高等级和更加面向后果的品质因素。概率风险评估需要的资源依赖于后果重要度模型，同时依赖于根据预期收益做进一步分析所需要的实时费用和资源。

NASA 的安全和风险指导书决定风险评估的范围和严格程度。NPR8715.3《NASA 通用安全性工程需求》根据后果类型和其他标准为项目分配优先序。NPR8705.5《NASA 工程和项目概率风险评估技术规程》根据优先级和设计成熟度确定评估范围、严格程度及评估细节。

1) 量化

每个备选方案的技术性能指标被量化，用来量化备选方案的全局性能指标体系或全局效能指标。这些量化结果用来为备选方案排序。

定界方法通常用来初步筛选可能的风险因素。然而，最终必须对风险诱因实施实际评估。定界方法不适合为备选方案排序，因为每个方案与其应用的技术性能指标之间存在偏差，很难做到在定量的一致性水平上逐个排序。

由于不同的工具使用不同的简化和近似，如果分析结果来自于不同的工具或不同的分析人员，很难以一致的方式对它们进行对比。在做工作计划或应用结果时，需要考虑不一致性的来源。认真评议的好处是能够留意这些因素影响下的风险与技术性能指标审查结果（见下文）。

2) 对不确定性缩减指标的考虑

在某些情况下，备选方案初步排序并不完备。鲁棒的排序应当对模型参数和假设的微小变化并不敏感。例如，假设不同决策备选方案的技术性能指标差异充分小，而在不确定性规定范围内关键参数的变化可能改变方案排序。这可能在某些决策情况下发生，包括架构决策和给定架构下的风险管理决策。在后一种情况下，不同的备选方案将导致不同的风险缓解方法。

针对这种情况，值得在减少不确定性的工作上投入。量化“信息的价值”可以帮助决策者决定减少不确定性是否是一个有效的资源利用。

4. 评议和推荐决策方案

1) 评议

为了运用集体智慧促进实际执行方案的选择，建议使用评议方式，或在复杂的和事关重大的决策情况下，建议进行最终权衡研究和不确定性缩减工作，如图 6.4-9 中“分析”箭头所示。

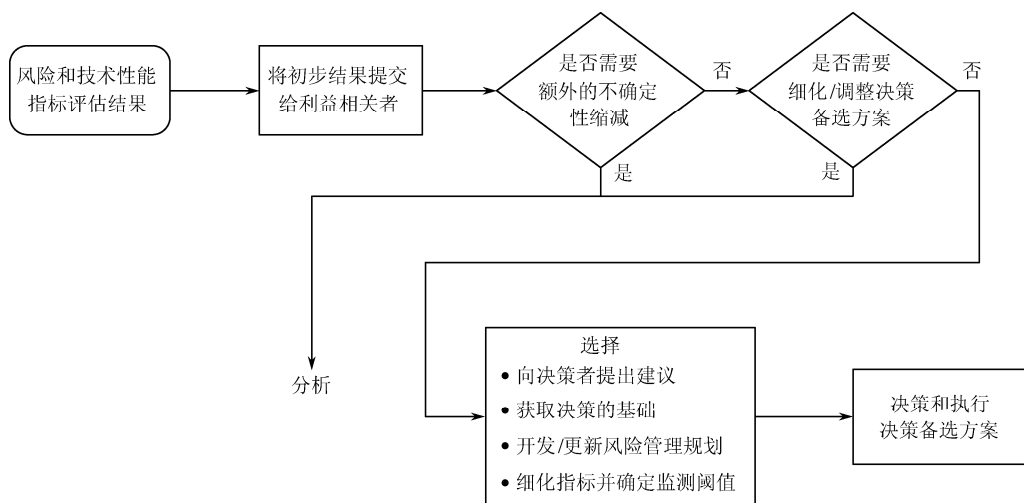


图 6.4-9 评议流程

2) 获取偏好方案及其选择基础

根据该方法的应用实践层级（项目层、子任务层等），在适当程度评议的基础上，技术团队选择一个备选方案。决策由系统工程流程内部相应的权威机构做出。实施这一步的目的是为了强调需要抓住备选方案的关键信息，该关键信息包括所感知的作为持续风险管理中规划活动输入的潜在工程漏洞。确切的说，备选方案的选择至少是部分基于对技术性能指标值的期望结果。为了监测和实施的目的，这些技术性能指标值可帮助定义成功准则，同时这些指标值决定监测阈值的关键输入。

3) 选定方案的技术风险管理计划

此刻单一方案已经选定。在分析过程中，为了量化技术性能指标，对每个备选方案的风险进行评估，但详细的风险管理计划并没有制定出来。在此阶段，需确定选定方案的技术风险管理详细计划，起草正式的风险管理计划。在计划阶段的工作包括如下：

- 作出风险控制（消除、减缓、研究、观察或接受）行动的临时决策；
- 确定观测值，用来度量工程性能；

- 确定观察值的阈值，不超过阈值表明满意的项目性能；
- 确定指导观测值测量频率、超过阈值时如何处理、决定分析更新的频率及决策机构等内容的协议；
- 分配风险跟踪的责任。

这里概述 NPR 8000.4《风险管理技术规程需求》中的风险控制行动通用分类。每个被识别和分析的风险可以用下列 5 个方法之一管理：

- 消除风险；
- 减缓风险；
- 研究风险；
- 观察风险；
- 接受风险。

如果很好地了解风险并且收益与成本相称，应采取措施以消除或减缓风险。收益通过运用工程目标层次的技术性能指标确定。需要分析减缓备选方案风险的后果以确保这些后果不会引起新的不必要的风险因素。

如果风险减缓不可行，需要考虑其他措施。假设有与风险相关的重大不确定性。例如，想定的风险概率或后果中可能存在的不确定性。这造成缓解效益的不确定性，这样就无信心做出风险减缓决策。在这种情况下，可能需要进行研究，以减少不确定性，更明确地指出合适的控制方法。研究只是个过渡措施，最终导致决定减缓风险或接受风险。

如果风险减缓和研究都不恰当，且风险相关的后果很小，则可能需要接受风险。风险接受流程需考虑后果的或然率和严重程度。NPR 8000.4 界定了工程层次接受风险的权威机构，并要求对接受的风险进行（至少每 6 个月一次）的定期评审，以确保条件和假设没有变化到需要重新评估所接受的风险。这些评审应适当采取定量和定性分析方式。

其余是那些无法合理采用风险减缓和研究，而风险相关的后果又有较大的情况。如果风险存在很大的不确定性，可能需要对它进行观察。这样可以在不专门针对此类风险开展工程研究的情况下，使不确定性随着项目推进和知识积累自然地减少。与研究相同，观察是过渡措施，根据既定的指导方针，逐渐导向风险缓解或接受风险。

4) 有效的计划

本小节讨论的首要目标是确保风险监测计划的实施获得净收益。

好的计划能够以适时方式高概率检测出工程中的显著偏差，而不会给工程带来额外负担。为了实现这一点，需要确定观测量和阈值的完整组合。精心选择计划并实施，检查实际技术性能指标值对技术性能指标计划值的偏离，通过这样做增加项目挣值，而不会提出需求增加项目负担。计划的内容包括某种程度上预先确定的财务和进展报告需求，以及附加的工程特有的观测量、审核和工程评审。

可观测量和阈值的选择应具有以下特点：

- 可度量参数（直接度量参数或可用于计算该度量参数的相关参数），用于根据明确的定义和客观的阈值对系统性能进行监测；
- 设置监测程序，这样当观测量超过阈值时，就能及时提供性能问题的指示；
- 这项活动的相关工程负担至少需要满足上述关于负担的要求。

例如，一个特定使命任务的损失概率不能直接度量，而是取决于许多此刻能够度量的量值，如较低层次的可靠性和可用性指标。

建立监测协议，其中阐明监测要求、分配监测责任、确立监测区间。收集和分析监测结果，并且在性能超出阈值时触发响应。这些协议还确定何时必须重新进行分析。例如，如果工程的目标发生变更，技术风险管理决策应当予以重新评估并进行分析。由于 NASA 工程要求的高技术产品需要长时间的开发，在工程寿命周期结束之前，工程需求经常发生变更。这些变更可能包括技术需求、预算或进度表、风险承受能力等。

5. 跟踪和控制性能偏差

如图 6.4-10 所示，风险跟踪是根据风险管理计划对其中的参数进行观察、编辑和报告的过程。当性能超出阈值时，如果发现被假设为微不足道的风险影响重大，或发现分析中未重视的风险，即启动风险减缓/风险控制流程。如果工程有显著变更，可能也需要进行风险控制。针对工程变更需要使用的风险控制指标在风险管理计划中决定。提出备选方案并进行分析，并且基于与技术性能指标、敏感性和不确定性分析及利益相关者评议等有关方案性能选择偏好方案。这样，新选定的偏好方案成为风险规划、跟踪和控制的主体。

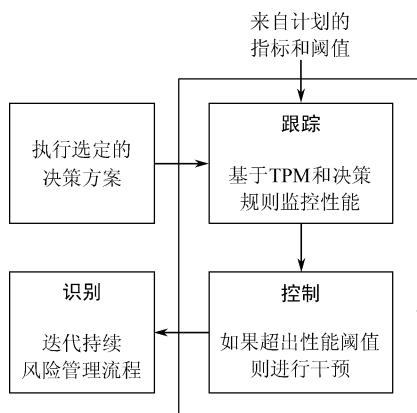


图 6.4-10 性能偏差监控

在计划阶段，风险控制备选方案在提出要求之前开始构想。一旦触发阈值，则要求执行风险控制行动（如 6.4.2.3 节所描述）。在此刻，可能有比在控制备选方案中提出的还要多的信息提供给决策者。因此，在对现有备选方案进行技术风险管理流程迭代之外，应当考虑新的备选方案或现有备选方案的修改。

图 6.4-11 给出根据预定的阈值跟踪技术性能指标余量来跟踪和控制性能的例子。在与纵向断点对应的时刻，技术性能指标余量小于要求的值。在这个点上，备选方案改变，这样余量和余量需求增大。

尽管活动的层次根据寿命周期中当前活动的位置发生变化，在工程结束之前，技术风险管理不能终止。主要输出是技术风险报告，包括提交备选方案的相关风险、风险控制方案及决策支持数据。随着获得更多关于方案的风险信息，风险控制方案反馈到技术规划。这一持续到风险管理计划建立。这个学习过程也会产生反馈到项目的方案、观点、问题和支撑数据。一旦选定项目的控制基线，技术风险管理关注的重点成为度量项目风险相对于控制基线的偏差，并形成基于这些度量值的决策支持要求。

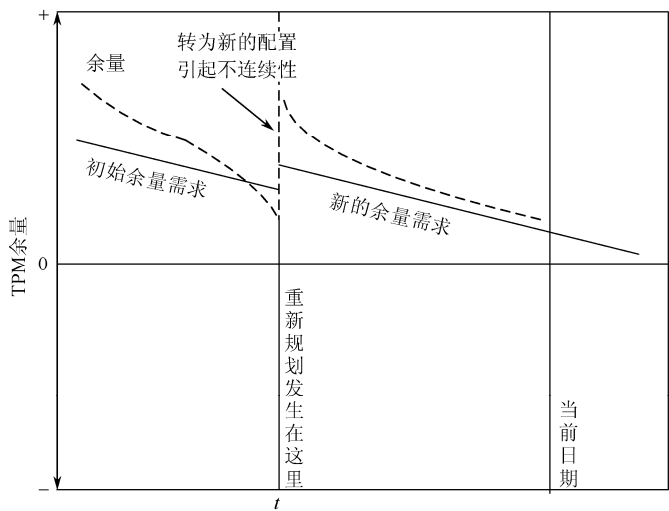


图 6.4-11 余量管理方法

6.5 技术状态管理

技术状态管理是在产品寿命周期内应用的，控制性能变更和功能与物理特性变更，并为其提供可视化的管理手段。技术状态管理保证产品技术状态是已知的并能反映产品的信息，任何产品变更是有利的且没有不良后果影响，并保证这些变更是可控的。

技术状态管理通过保证正确的产品技术状态降低技术风险，区别不同产品的版本，确保产品和产品信息之间的一致性，并避免出现利益相关者不满和投诉的尴尬。NASA 采用在 ANSI/EIA 649 中定义的技术状态管理原则，采用由 NASA 技术状态管理专业人员定义并被 NASA 管理层批准的实施方法。

当应用到设计、制造/组装、系统/子系统试验、集成、使用和维护等复杂的技术活动中时，技术状态管理代表工程组织和计划结构的脊梁。它逐步建立原则并保持产品属性和文档的一致。技术状态管理使所有相关技术工作者，在产品寿命周期任意时刻的开发和决策过程中使用完全一致的数据。技术状态管理的原则适用于保持文档与已批准的工程过程一致，确保产品符合经批准设计的功能和物理需求。

6.5.1 流程描述

图 6.5-1 给出了技术状态管理流程的典型流程图，并给出技术状态管理中应该考虑的典型输入、输出和活动。

6.5.1.1 输入

该流程所需要的输入如下：

- 技术状态管理计划；
- 待控制的工作产品；
- 提出的控制基线变更。

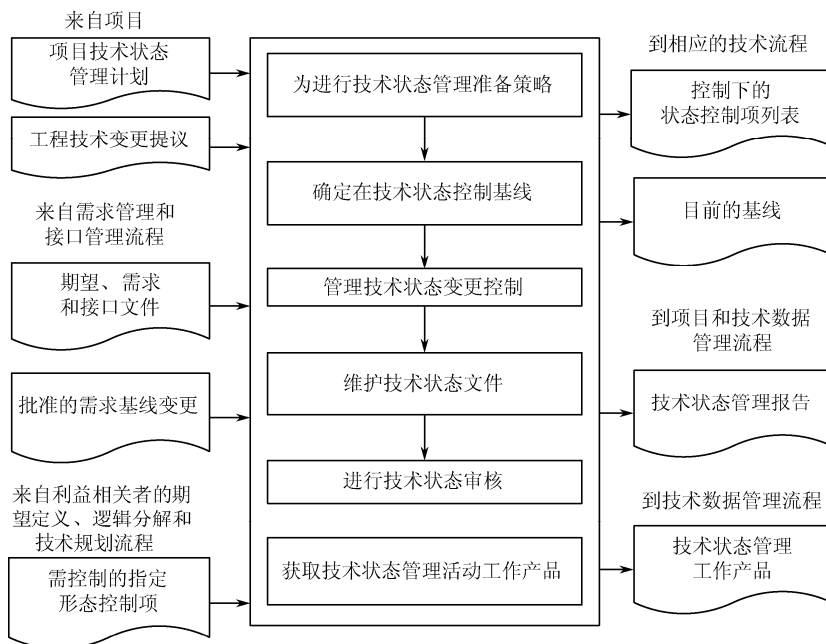


图 6.5-1 技术状态管理流程

6.5.1.2 流程活动

技术状态管理有如下 5 个要素（见图 6.5-2）：

- 技术状态计划和管理；
- 技术状态识别；
- 技术状态变更管理；
- 技术状态状况记录；
- 技术状态验证。

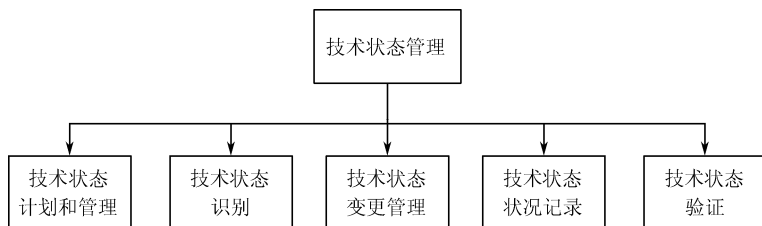


图 6.5-2 技术状态管理的 5 个要素

1. 技术状态管理的计划与管理

技术状态管理计划始于工程或项目的初期。技术状态管理办公室必须在技术状态管理工具或承包商技术状态管理监督中仔细权衡资源排序的价值。NASA 中心技术状态管理组织的评审是必要的而又花费资源和时间的，但在技术状态失控爆发之前更正技术状态管理的系统问题，总比解释为什么错误的或误认的部件会造成工程/项目中的重大问题要好。

准备实施技术状态管理的关键输入之一是项目技术状态管理完整流程的战略计划。这通常包含在技术状态管理计划中。典型技术状态管理计划大纲参见附录 M。

这个计划的内部和外部作用如下所述。

- **内部作用：**项目办公室用来指导、监督和度量整个技术状态管理流程。它同时描述为后续采办阶段计划的技术状态管理活动和实施这些活动的进度表。
- **外部作用：**技术状态管理计划用于与工程涉及的承包商沟通技术状态管理流程。它建立一致的技术状态管理流程和工作关系。

技术状态管理计划可以是一个独立的文件，也可以和工程的其他计划文件相结合。它应描述每个技术控制基线产生、技术审批和审核的标准。

2. 技术状态识别

技术状态识别是选择、组织和陈述产品属性的系统性过程。技术状态识别需要为产品及其技术状态文件赋予唯一标识。与技术状态识别有关的技术状态管理活动包括选择状态控制项，确定状态控制项相关的技术状态文件，确定适当的变更控制权限，为状态控制项和状态控制项文件分配单一标识，发布技术状态文件，并建立技术状态控制基线。

NASA 有四个控制基线，分别定义产品设计进展中界限清晰的阶段。控制基线针对公认的状态控制项，确定其在某个时刻点上的属性描述，并为其处理变更问题提供已知的技术状态。控制基线在状态控制项属性的陈述定义被认可（和记录）时建立。经批准的“当前”控制基线成为定义后续变更的基础。系统规范通常在系统需求评审之后最终定稿。功能控制基线在进行系统定义评审时建立并通常同时转为由 NASA 控制。

通常由工程、项目或 NASA 中心控制的四个控制基线（见图 6.5-3）如下所述。

- **功能控制基线：**功能控制基线是被批准的技术状态文件，它描述系统的或顶层状态控制项的（功能性、互操作性和接口特性）性能需求，描述为证明这些指定的特性已经达到而需要进行的验证。功能控制基线由 NASA 控制。
- **配定控制基线：**配定控制基线是被批准的面向待开发状态控制项性能的技术状态文件，它描述从高层需求文件或状态控制项分配的功能和接口特性，同时描述为证明这些指定的特性已经达到而需要进行的验证。配定控制基线将功能控制基线的顶层性能需求扩展到足够详细程度，以启动状态控制项的制造或编码。配定控制基线通常由设计部门控制，直到所有的设计需求被证实已设计实现。配定控制基线通常在初步设计评审圆满完成时建立。在进行关键设计评审之前，伴随工程数据的不断发布，NASA 正式评审设计输出是否符合设计需求。NASA 通过对工程数据内容的评审形成对配定控制基线的控制。
- **产品控制基线：**产品控制基线是被批准的技术文档，它描述在产品寿命周期中的生产、安装/部署和使用保障阶段状态控制项的技术状态。所建立的产品控制基线的控制由在阶段 A 开发的技术状态管理计划中描述。产品控制基线通常是在完成关键设计评审之后建立的。产品控制基线描述以下内容。
 - 状态控制项的详细物理特性或形状、组装和功能特征；
 - 为生产验收试验选择指定的功能特点；
 - 生产验收试验的需求。
- **部署控制基线：**部署控制基线出现在进行运行使用准备状态评审时。在这一时刻，设计可以被认为已实现功能并完成飞行准备。所有变更都将被记录在文件中。

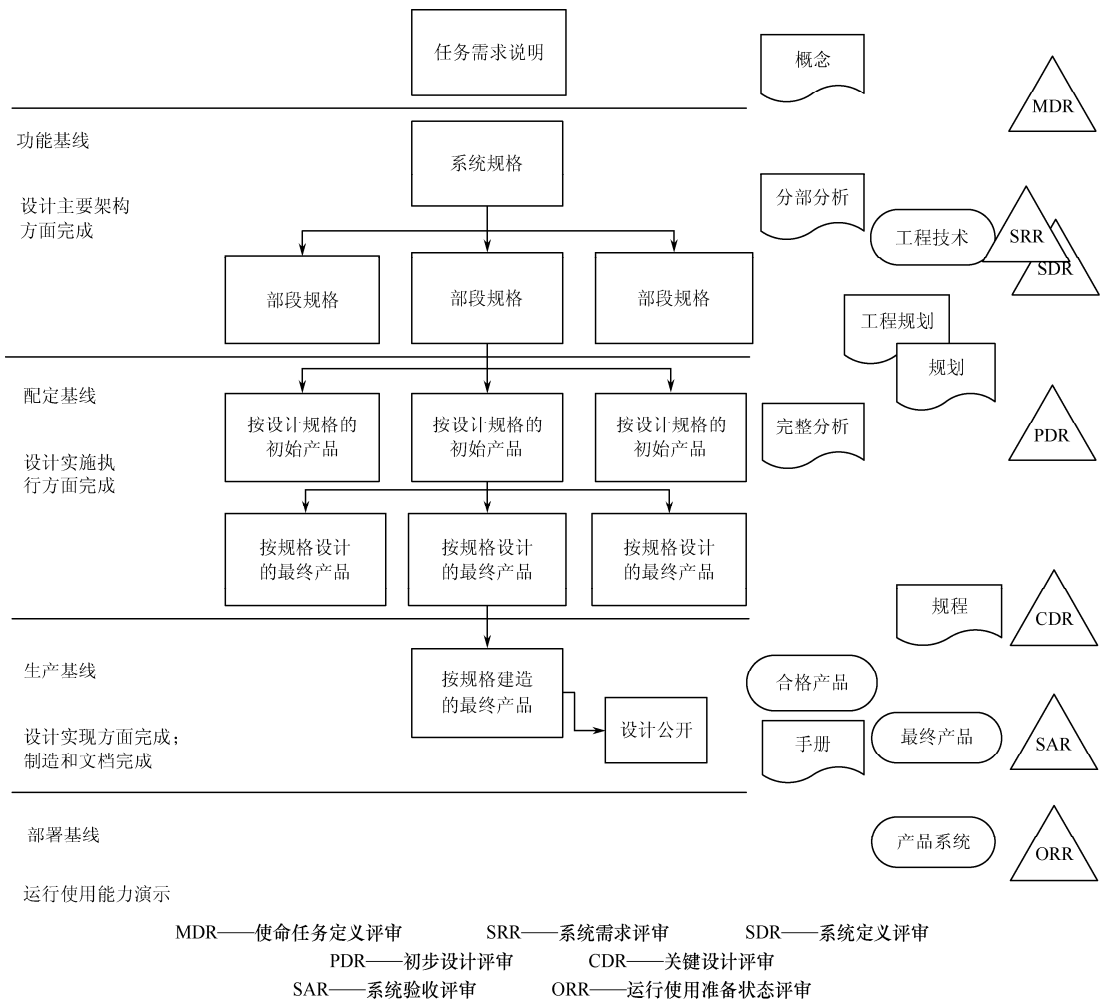


图 6.5-3 技术控制基线的演化

3. 技术状态变更管理

技术状态变更管理是管理已批准设计和实施已批准变更的过程。技术状态变更管理通过系统地提出变更、论证和评估提议的变更、归并提议的变更和验证变更实施的结果来实现。在特定的工程中实施技术状态变更管理，需要有该项工程目标和需求的专门知识。第一步是建立一个强有力的和经验丰富的 NASA 内部技术状态控制委员会体制，由工程变更权威部门的人员领导。技术状态控制委员会成员代表利益相关者，根据授权组织代表其利益的团队。第二步是形成对承包商活动的技术状态变更管理监督。技术状态管理办公室向 NASA 工程或项目负责人提出建议，以达到技术状态变更管理实施的平衡，适应工程/项目特有的情况。典型技术状态变更管理控制流程的示例如图 6.5-4 所示。

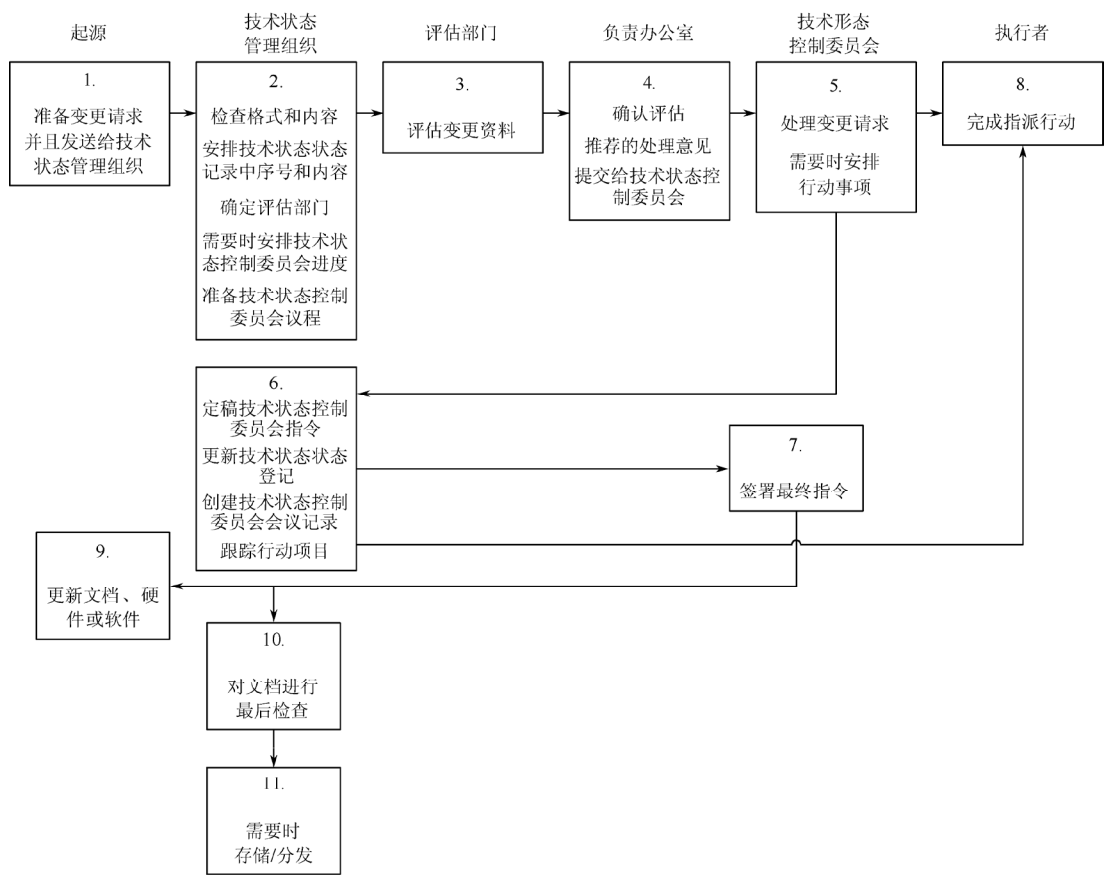


图 6.5-4 技术变更控制流程

技术状态变更管理中变更的类型

- **工程技术变更：**工程技术变更是在（草案中或已建立的）控制基线内的迭代。变更可以是主要的或次要的。其中可能包括也可能不包括规范的变更。影响外部接口的变更必须与所有受影响的利益相关者协调并获得批准。
 - “主要”变更改变控制基线技术状态文件，具有重大的影响（即需要更新改造已提交的产品，或影响与产品相接的其他产品、操作人员和维护训练的控制基线的规范、成本、安全和兼容性）。
 - “次要”变更更正或修改技术状态文件或流程，而不影响产品的互换性或系统结构中的系统要素。
- **免责声明：**免责声明是有意放松对工程或项目满足需求要求的协议文档（某些中心在产品的设计实施执行前使用变更声明，而在实施执行中使用免责声明）。经审定的免责声明不在控制基线变更内。

4. 技术状态状况登记

技术状态状况登记是有效管理状态控制项需要的技术状态数据记录和报告。有效的技术状态状况登记系统提供及时和准确的技术状态信息，例如：

- 完整的当前和历史技术状态记录及唯一标识。
- 提出的变更、变异和免责，从开始到实施的状况。

- 已辨识差异的状况和最终处置，以及在每个技术状态审核中识别的行动。

技术状态状况登记数据的部分目的如下：

- 辅助评价提议的变更，辅助变更决策，对设计中的问题、保证书、保质期计算进行调查。
- 历史可追溯性。
- 软件故障报告。
- 性能指标数据。

在设计和购买辅助管理技术状态任务的软件时，需要考虑的关键功能和属性如下：

- 实时地与内部、外部利益相关者安全共享数据的能力；
- 版本控制和比较（追踪软件或产品的历史）；
- 安全的用户登出和登录；
- 信息的跟踪能力（即时间、日期、人员、时间段等）；
- 基于网络的能力；
- 通过电子邮件发放通知的能力；
- 集成其他数据库或已有系统的能力；
- 与必要的承包商及/或供应商兼容的能力（即如果需要可从第三方接收数据）；
- 按照要求集成草图阶段和编制阶段的程序；
- 为用户提供中立格式浏览器；
- 允许商定数目范围内多用户的许可协议；
- 工作流管理和寿命周期管理；
- 有限的用户定制；
- 持续支持软件升级；
- 用户界面友好；
- 考虑用户的有限访问；
- 将计算机上标准格式文件作为附件的能力；
- 工作流能力（基于特定的标准集排列状态控制项）；
- 能够且唯一作为信息发布源的能力。

5. 技术状态验证

技术状态验证通过检查文件、产品和记录，通过评审技术规程、流程和业务系统来验证产品是否已达到所需的性能需求和功能属性，并通过验证产品的设计是否已形成文档来完成。这项工作有时分为功能的和物理的技术状态审核（有关技术评审的更多细节参见 6.7 节）。

6.5.1.3 输出

NPR 7120.5 按阶段进展定义了项目寿命周期。从 A 前阶段开始，这些阶段依次在规划论证和实施执行标题下分组。在这些阶段之间转换需要审批。采用关键决策点来定义阶段之间的转换。技术状态管理的作用是确定关键决策点是否达到。技术状态管理的主要输出是技术规程、批准的控制基线变更、技术状态状况和审核报告。

6.5.2 技术状态管理指南

6.5.2.1 不做技术状态管理的影响

不做技术状态管理的影响是可能导致项目被混乱、不准确、低效率和难以处理的技术状态数据所困扰。在哥伦比亚号^①事故调查中，事故调查委员会发现事故的发生与相关硬件和归档文件中“未协调并记录”的变更之间存在不一致有关。而此前技术状态管理问题没有被认为是事故原因。通常不执行技术状态管理的影响可以描述为“技术状态失控”。在 NASA 内部，这将导致工程延期和工程技术问题，尤其是在（如 X-37 工程^②）快速原型开发中，进度表比硬件工作记录拥有更大的优先权。如果技术状态管理正确实施，在功能和物理技术状态审核中其中差异将得到处理。

警告牌/红色标志（你怎么知道你有麻烦了？）

技术状态管理不当实施的一般警告标志如下：

- 工程中定义“顶层”技术需求失败（“我们不需要规范”）。
- 工程中在设计评审之前和之后的认定控制基线活动失败。
- 工程办公室将评估工程变更的时间减少到工程技术、安全与使命任务担保或其他技术状态控制委员会成员不可能完成这项工作的水平。
- 工程办公室宣布在技术状态控制委员会文件中的“记录没有异议”。
- 工程办公室在没有技术状态管理组织同意的技术状态管理需求支持情况下拨付合同款。
- 追踪设计变更的生产底线时不当使用红线。
- 材料评审委员会不知道关键的、主要的和次要的不一致性之间的差别和免责声明的适当分类。
- 图纸质量不高且没有包含适当的说明以确定技术状态控制或适当容错的关键工程项目。
- 供货商不了解针对工程中定义的安全性需求提交免责声明的含义。
- 分包商/供货商未经上级承包商批准更改工程设计，不知道如何协调和编写工程变更请求等。
- 制造加工技术没有与工程变更保持一致，影响了加工质量。制造工具失去技术状态控制和生产可接受性。
- 验证数据不能追踪到为验证任务应用而发布的部件编号和规格。
- 使用手册及维修指令中不能追踪到为维修/改装任务应用而最新发布的部件编号和维修图纸。
- 维修和地面保障工具及设备无法追踪到适用于设备的最新发布的部件编号和规格。
- 部件和构件因不当识别标记而无法确定。
- 数字的任务完成影像不能关联到最新发布的工程产品。
- NASA 无法通过访问承包商的技术状态管理网站验证最新发布的工程产品。
- 每项安装技术规程需要的工具与状态控制项设计中使用的紧固件和螺栓螺帽不匹配。
- 由于在运输和包装容器设计中缺乏技术状态控制，状态控制项与其包装箱和容器不匹配。
- 支持采购/制造变更的技术规程没有充分取得工程技术组织的认可。

以下是以往可能或已经发生的影响：

- 由于硬件或软件的不当配置或安装导致使命任务失败和财产生命损失；

① “哥伦比亚”号航天飞机是美国天地往返运输系统的首件正式产品，1981 年 4 月 12 日在美国佛罗里达州卡纳维拉尔角发射升空。哥伦比亚号曾 17 次执行空间运输和科学实验任务。2003 年 2 月 1 日在执行任务后返回地面时，因高温气体从发射时被脱落的泡沫材料击中的左翼隔热板缝隙进入机体而导致其内部结构融化，最终解体坠毁。

② X-37 是美国国防和 NASA 为实现“快速全球打击”构思而研制的一种空天飞机。

- 由于硬件或软件的不当配置或安装导致收集使命任务数据失败；
- 由于硬件或软件的不当配置或安装导致使命任务重大延误而增加额外成本；
- 由于采用虚假验证数据使得部件或者子系统被不恰当认证而造成使命任务费用增加或重大延误。

如果技术状态管理实施不当，可能会在制造、质量、接收、采购等方面出现问题。如果不维护综合后勤保障数据，用户也将遇到问题。使用能够安排和跟踪任务的共享软件系统可以为团队提供项目成功的必要资源。

6.5.2.2 在什么时候使用红线图可以接受

“红线”是指在设计、制造、生产和试验中对发现有错误或不准确之处的图纸和文件进行标记的控制过程。如果文件需要通过正式变更流程进行纠正则可能导致停工。

所有红线至少要获得负责硬件的管理人员和质量保证管理人员的认可。这些管理人员决定这些红线是否要纳入计划或技术规程。

重要的是，每个项目必须有一个红线控制技术规程来指定红线确定和批准程序。

作为 NOAA N-Prime 灾难^①的主要原因之一的红线

摘自 NOAA N-Prime 灾难调查的最终报告：

“几个因素促成了 NOAA N-Prime 事件，其中最重要的是缺乏适当的多次反复验证，其他包括缺乏适当的产品担保证书，进度表变更并对操作人员构成影响，在清理接口界面时操作人员没有注意螺栓已卸除的失误，没有及时或根本没有通知安全部门、产品担保和政府的代表，以及不当使用红线技术规程导致难以处理事件发展。几个因素的相互作用导致如此情况，经验极其丰富的雇员没有留意手中的活动。这样就错过了可能避免灾难的机会。

“此外，该操作团队面对使用需要在相当多的步骤之间极频繁“跳跃”的红线技术规程，而此前从未演练过。书写糟糕的技术规程和全新的红线成为负责测试的工程师做出错误决策的前提。

“集成和试验主管同意了执行测试不足的文件和技术规程红线的不当使用。

“关键流程被发现不合适，包括那些规范了操作节奏、使用计划、技术规程开发、红线使用和地面保障设备技术状态的流程。例如，在事故发生时需要广泛使用红线技术规程。这些技术规程从使用上来说说是全新的，也就是说，在之前的操作中从未在如此特殊的实际情况中使用过。尽管这样此前从未发生过广泛使用红线，但改写后的技术规程通过相应的渠道被批准了。在批准过程中并没有进行危险和安全性分析。”

6.6 技术数据管理

技术数据管理流程用于技术数据的规划、获取、访问、管理、保护和使用时，以支持系统的全寿命周期。按照 NPR1441.1 《NASA 记录保存计划》的要求，数据管理包括使命任务和科学方面技术数据的开发、部署、运行、维护、最终退役，以及系统退役后的数据留存。

数据管理流程如图 6.6-1 所示。数据管理的系统工程方面主要内容包括如下：

^① NOAA N-Prime 是美国洛克西德马丁公司为 NASA 制造的第 5 颗新一代系列环境卫星，2003 年 9 月 6 日，该星在制造平台上将姿态调整到水平位置时，因为操作人员未注意固定螺栓已经移除而造成卫星直接坠落地面，为此造成 1 亿 3500 万美元的损失。2009 年 2 月 6 日，该星发射升空，在成功进入预定轨道后被更名为 NOAA-19 卫星。

- 数据鉴别和控制的策略与技术规程应用；
- 及时、经济地获取技术数据；
- 数据及数据保护的充分性保证；
- 使用时便于对数据进行访问和分发；
- 数据使用的分析；
- 数据对于未来其他工程/项目价值的评估；
- 对记录在已有软件中的信息处理访问。

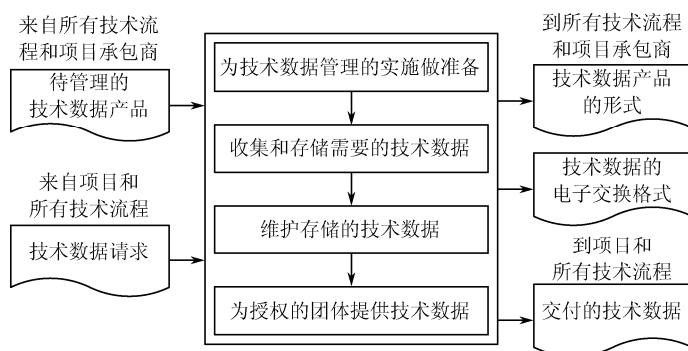


图 6.6-1 技术数据管理流程

6.6.1 流程描述

图 6.6-1 给出了技术数据管理流程典型的流程图，并给出技术数据管理应考虑的典型输入、输出和活动。

6.6.1.1 输入

输入包括技术数据，不考虑数据格式和记录方法，不考虑待开发系统寿命周期中，数据是由承包商还是政府生成。技术数据管理流程的主要输入如下：

- 工程数据管理计划；
- 待管理的数据产品；
- 数据访问请求。

6.6.1.2 流程活动

NASA 中心负责技术数据管理的政策和技术规程。NPR7120.5 和 NPR7123.1 定义了管理数据的需求，但将细节留给中心。然而，NPR7120.5 要求提供数据管理计划，作为工程/项目计划的一部分或单独文档。工程或项目负责人确保能够获取和存储所需数据、维护数据完整性并按需要分发数据。

数据的获取和存储问题由其他 NASA 政策解决，这些政策不仅仅局限于系统全寿命周期内的技术数据。

1. 数据管理计划的作用

推荐的技术规程是数据管理计划作为从工程/项目计划中分离出的独立计划。独立计划中

对数据管理问题的判定非常重要。NASA 政策和技术规程中未特别指定相应特性而为更详细的数据管理计划提供进一步支持。该计划应该覆盖的主要数据管理主题如下：

- 对产品寿命周期所有方面数据需求的标识/定义。
- 控制技术规程——接收、修改、审查和批准。
- 关于用户如何访问、搜索数据的指南。
- 能够促进数据重用，有助于确保数据在系统、族系或者体系中使用的一致性的数据交换格式。
- 数据的权限和分发限制，例如，敏感但不涉密信息的输出控制。
- 数据的存储和维护，包括描述文档和记录的维护与管理的总清单。

2. 技术数据管理需考虑的关键事项

接下来的活动是搜集、存储和维护技术数据，并按需要提供给经授权的团体。影响实施这些技术数据管理活动需考虑的事项如下：

- 与承包商之间数据流/发送的相关需求应该在技术数据管理计划中说明，并且包含在申请指南和承包商协议中。
- NASA 不会强行要求承包商变更现有数据管理系统，除非工程技术数据管理需求（包括数据交换需求）不能满足。
- 数据输入到技术数据管理系统的职责完全依赖于数据的构造者或生成者。
- 技术数据的使用/访问依赖于数据的创作者、构造者或生成者，以及技术数据管理系统的管理人员。
- 建立的使用/访问描述和列表应该在技术状态控制下确定控制基线和处理。
- 对于新的工程，需要数字化的数据生成和发送方法。已有工程必须权衡硬拷贝数据数字化的费效比。

3. 数据管理的一般作用

技术数据管理流程提供政策和技术规程的应用基础，支持辨识和控制数据需求，快速经济地获取、访问和分发数据，以及分析数据的使用。

坚持数据管理的原则/规则能够在政府和工业部门的技术工作中实现数据的共享、集成和管理，并确保所管理的技术数据生成满足要求或者达到期望的信息。

技术数据管理流程对获取和组织技术数据起引导作用，并为下列应用提供信息：

- 辨别、收集、存储和维护产生于其他系统工程技术流程和技术管理流程工作产品，以及形成这些工作产品过程中做出的假设。
- 促使系统产品数据的协同和全寿命使用。
- 获取和组织技术工作输入，以及当前的、中期的和最终的输出。
- 存在于需求、设计、解决方案、决策和基本原理之间的数据相关性及其可追溯性。
- 记录工程技术决策，包括技术规程、方法、结果和分析。
- 产品再次购买和产品保障时促进技术引入以提升购买力。
- 需要时，支持其他技术管理和技术流程。

4. 数据标识/定义

在每个工程/项目的寿命周期中确定数据需求。数据类型可以在标准文档中定义。NASA

及其中心的指导书有时指定文档内容，并相应地用于内部数据准备。标准描述可能被修改以满足工程/项目的特定需求，在任务书中可能需引入适当的描述语言来实施数据评估引起的活动。“数据供应者”可能是承包商、学术界或政府部门。从外部供应者那里采购数据是正式活动，需要采购文档，内部需求可能以非正式方法处理。下列是可能用于工程/项目的不同数据类型。

- **数据：**
 - “数据”通常定义为“不考虑格式或方法的信息记录”。然而，术语“数据”和“信息”经常互换使用。精确地说，数据通常经过某种方式处理后生成有用的、有价值的信息。
 - 系统工程数据管理中的“数据”，包括技术数据、计算机软件文档，以及事实、数字或任何具有可交流、存储和处理特性的数据描述；如此形成合同或协议需要的信息，交付到政府部门或被政府部门访问。
 - 数据包括系统开发、用于开发或试验的建模和仿真、试验与评价、安装、部件、备件、维修、产品维护所需数据，以及数据源或提供者提供的数据。
 - 明确不包括在技术数据管理内的数据是那些与 NASA 劳工业务信息相关的数据、通信信息（除了与特定需求相关）、财务事项、个人数据、交易数据，以及其他纯粹商业性质的数据。
- **数据清查：**来自政府部门相关人员（特别是集成产品小组的领导和职能负责人）的请求，确认和证明来自采购合同的数据需求。由于承包商提供的数据由政府负担费用，数据清查（或等价行为）是一种常规控制机制，用于确保要求的数据确实被需要。如果通过数据清查证实，则开发每个需要的数据项描述并在合同中注明。
- **信息：**信息通常被认为是处理过的数据。处理数据的方式依赖于可用的文档、报告、审查的形式或模板。
- **技术数据包：**技术数据包是相应支持采办策略、生产、工程技术和后勤保障的数据产品技术描述。数据包定义所需要的设计技术状态和技术规程以确保数据产品性能的充分性。数据包由所有可用数据产品组成，例如，图纸、清单、规范、标准、性能需求、品质保证规定和包装细节。
- **技术数据管理系统：**管理工程技术数据所需要的策略、计划、技术规程、工具、人员、数据格式、数据交换规则、数据库，以及其他实体和描述。

技术数据的不当使用

技术数据的不当使用示例如下：

- 涉密数据或通过秘密渠道提供的数据未经授权而泄漏；
- 基于不完整、脱离背景或者易误解数据做出的错误解释；
- 在必须但未获得政府部门授权的部件采购或维护中使用数据。

帮助防止技术数据的不当使用的方法如下：

- 在相应数据使用方面培训利益相关者；
- 控制数据的访问权。

5. 数据管理系统的初始结构

在建立数据管理系统时，不需要获取（即购买和要求提交）项目生成的所有技术数据。

基于按需了解的可访问性，某些数据可能存储在其他位置。只有当访问权不够充分、及时或安全而无法提供敏捷的寿命周期计划和系统维护时，才应当购买数据。数据清查是处理该需求的通用控制机制。

6. 数据管理计划

- 准备技术数据管理策略。这个策略能够记录工程数据管理计划如何通过技术努力实施，或在缺少这样的工程层计划时，如何用做准备详细技术数据管理计划的基础，包括如下：
 - 根据工程或组织的策略、协议或法规来管理的数据项；
 - 数据内容和格式；
 - 工程内部及与承包商之间的数据流框架，包括技术工作信息交换使用的语言；
 - 与数据产品的来源、生成、获取、存档、安全、保密和处置相关的技术数据管理职责和权限；
 - 为数据项的保留、传播和访问而建立的权利、义务和承诺。
 - 依据工程或组织的策略、协议和法规约束条件而使用的相关数据存储、转换、传播和表现的标准和惯例。
- 从相应的利益相关者处获得策略/计划承诺。
- 为实施针对技术工作的技术数据管理策略，并为实施技术数据管理计划的活动准备技术规程。
- 建立技术数据库，用于技术数据维护和存储，与工程人员合作为技术数据管理安排工程数据库的使用。
- 建立适用于技术数据管理范围和可用资源的数据采集工具（见 7.3 节）。
- 根据国际标准/协议和可用的 NASA 标准，建立电子数据交换接口。
- 可能时在建立技术数据管理策略/计划、技术规程和数据采集工具的同时，培训相应的利益相关者和其他技术人员。
- 期望的结果如下。
 - 用于实现技术数据管理的策略和计划；
 - 建成的执行计划中技术数据管理活动的技术规程；
 - 待管理数据的总清单，按照种类和用途分类；
 - 建成可用的数据采集工具；
 - 能够指导建立技术数据管理技术规程和使用可用数据采集工具的合格技术人员。

7. 计划数据管理和工具选择需要考虑的关键事项

- 输入到技术数据管理系统和分发到系统数据库请求者的所有数据，应能追溯数据创作者、构造者或生成者。
- 所有输入到技术数据管理系统的技术数据应具有当前审批、协议和信息等状况的客观证据、版本/控制号和日期。
- 技术数据管理方法应该作为工程的系统工程管理计划的一部分。
- 期望用于部件采购和维护服务的技术数据，可能需要通过 NASA 中心法律顾问的审查。

在计划访问和存储项目或工程生成的数据时，需要细致考虑。如果需要系统或者工具，技术状态管理工具可被多次非正式使用。如果需要管理数据的独立工具，参见下节提到的评估数据管理工具的最佳实践案例。必须在数据访问权和数据输入权方面设置优先级。第二优先考虑的应该是针对当前工程/项目、未来的工程/项目、NASA 全局效率和 NASA 工程知识唯一性方面特定数据的价值。

如果需要设计或者购买软件来辅助管理数据任务，那么应考虑的关键功能或属性如下：

- 支持内部和外部利益相关者安全共享数据的能力；
- 版本控制 and 对比，用来追踪对象或产品的历史；
- 安全的用户更新；
- 直至文件级的访问控制；
- 基于网络的数据管理；
- 连接数据到技术状态管理系统或者单元的能力；
- 与承包商或供应商的支持兼容，即能够根据需要接收来自第三方的数据；
- 根据需要集成处于草案中和建模中的程序；
- 为用户提供中立格式的阅读器；
- 允许多用户的许可证协议；
- 工作流和寿命周期管理，此为建议选项；
- 有限的用户定制化；
- 软件版本升级时的多重支持；
- 用户界面友好；
- 直接搜索的能力；
- 将计算机标准格式文件作为附件的能力。

8. 数据的价值

工程数据的存储需要在项目或工程的开始阶段规划。有些数据类型只能在受控于 NPR1441.1 《NASA 记录保留计划》情况下使用；那些不受控的类型必须说明。最好是评估所有产生的数据，决定其对项目/工程或 NASA 工程技术整体上的价值。评价数据价值时需要询问的四个基本问题如下：

- 数据是否描述待开发或建造中的产品/系统？
- 开发建立的是精确制造产品/系统需要的数据吗？
- 数据能为增强未来相似的工程/项目的理解力提供支持吗？
- 数据是否具备需要在 NASA 的知识库中维护的关键信息，供工程师未来使用或作为学习案例保存？

9. 获取技术数据任务

表 6.6-1 定义了获取技术数据所需完成的任务。

表 6.6-1 技术数据任务

描 述	任 务	期 望 结 果
技术数据获取	<p>收集和存储来自技术流程和技术管理流程的输入和技术工作结果，包括如下：</p> <ul style="list-style-type: none"> 来自技术评估的结果； 使用的方法、工具和指标体系的描述； 建议、决策、假设，以及技术工作和决策的影响； 经验和教训； 计划的偏差； 相对于需求而言的异常和超差； 追踪需求的其他数据。 <p>对收集的数据执行数据完整性检查，确保内容和格式的一致性；同时进行技术数据检查，确保指定和记录的数据没有错误。向数据的创作者或生成者报告完整性检查中的异常或差异，以完成数据纠正。作为常规计划维护的一部分，对数据采集和存储的技术规程排序、评审和更新</p>	<p>需要用来执行和控制技术流程和技术管理流程的可共享的数据已采集和存储。</p> <p>存储数据的详细目录</p>
技术数据维护	<p>对收到的技术数据产品执行技术管理作用和职责。</p> <p>管理数据库，确保采集的数据有足够的品质和完整性，且相对拥有访问权限的人员是适当连续、安全和可用的。</p> <p>定期评审技术数据管理活动，确保一致性，并辨识异常和差异。</p> <p>评审存储的数据，确保完整性、充分性、有效性、可用性、精确性、实时性和可追踪性。需要时执行技术数据维护。辨识和记录重要问题、它们的影响，以及为改正问题和减轻影响对技术数据的变更。维护和控制存储的数据，防止其被不适当使用。以能够方便快捷恢复的方式存储数据。以某种方式维护存储的数据，保护技术数据远离可预见的危险，例如，火灾、洪水、地震等</p>	<p>技术数据维护记录。</p> <p>技术工作数据，包括获取的工作产品、承包商提交的文档和购货方提供的文档，均已被控制和维护。</p> <p>数据存储的状态被维护，包括版本描述、时间控制基线和安全等级</p>
技术数据/信息分发	<p>维护信息库或参考索引，保证技术数据可用性并提供访问指令。</p> <p>接收和评价数据请求，由此决定数据需求和传输指令。</p> <p>依据已建立的处理相关请求的技术规程，处理技术工作数据或信息的特殊请求。</p> <p>根据协议、工程指令、技术数据管理计划和技术规程，确保被要求和请求的数据能够适当地分发从而满足需求者和请求者的需要。</p> <p>在允许数据库访问或任何被请求数据以电子方式发布/传送到请求者之前，确保遵从电子访问规则。</p> <p>为提供给内部和外部接收者的技术数据提供正确性、可靠性、安全性证据</p>	<p>访问信息（如可用的数据、访问方式、安全技术规程、可用性时间窗口、明确的个人访问权限）确实可用。</p> <p>技术数据通过适当的格式提供给授权的请求者，包括适当的内容、安全的发送模式</p>
数据管理系统维护	<p>执行安全措施保护技术数据库和传送中的技术数据，防止未授权的访问和入侵。建立全局技术数据一致性的证据，促进高效的使用。适当地维护每个技术数据的备份。</p> <p>评估技术数据管理系统，确定采集和存储性能问题和难题；数据用户的满意度；数据延迟或毁坏的风险，未授权访问的风险或者信息从火灾、洪水、地震等意外中保存下来的能力。</p> <p>系统性地评审技术数据管理系统，包括数据库容量，决定其对国防采办框架后续阶段的适应度。</p> <p>对于发现的风险和问题，建议如下改进：</p> <ul style="list-style-type: none"> 作为技术风险管理的一部分，控制识别的风险； 通过建立工程变更管理活动来控制推荐的变更 	<p>当前可用的技术数据管理系统。</p> <p>技术数据适当地且有规律地备份以防止数据丢失</p>

10. 保护可交付使用的数据

所有可交付数据应该包括发布说明和技术规程，保护所有包含关键技术信息的数据，同时确保受限发布的数据、知识产权数据或所有权数据在系统工程活动中被适当处理。这项规定无论对硬拷贝还是数字化的数据都适用。

作为全部资产保护计划的一部分，NASA 建立了保护关键工程信息的特殊技术规程。关键工程信息可能包括组件、工程/设计/制造流程和技术、系统能力和弱点，以及任何展示系统独特的运行能力的其他信息。

关键工程信息保护应该是技术数据管理工作考虑的关键事项，是资产保护计划流程的一部分，见附录 Q。

数据采集检查清单

- 是否已确定采集的频率，以及技术流程和技术管理流程中可数据输入的时刻点？
- 是否已建立将数据从初始点移送到存储仓库或利益相关者的时间控制基线？
- 谁负责数据的输入？
- 谁负责数据存储、检索和安全？
- 是否已开发或采购必要的支撑工具？

6.6.1.3 输出

输出包括能够及时安全送达授权接收者的以各种形式表现的所需数据。

技术数据管理流程的主要输出如下（见图 6.6-1）：

- 技术数据管理技术规程；
- 数据表示形式；
- 数据交换格式；
- 分发请求数据/信息。

6.6.2 技术数据管理指南

6.6.2.1 数据安全性和国际武器交易规章（ITAR）

NASA 产生过非常庞大的信息，其中多数是非涉密和非敏感性的，信息使用和分发几乎没有限制。NASA 也通过大量工程、项目，以及与其他联邦机构、学术界和私人企业的协作，产生和维护涉密的国家安全信息。采用“敏感但非涉密（内部）”标记是要求创作者、发布者和接受者保持对敏感文档和数据的控制，或将控制权转交现成的控制流程。公开发布是禁止的，有此标识的文档/数据必须通过安全方式传送。安全方式有加密邮件、保密传真或单线追踪。WebEx 是不安全的环境。不允许用标准 E-mail 传送内部文档和数据。通过 E-mail 安全发送内部信息的方式是使用公共密钥基础结构传送文件。公共密钥基础结构是加锁/解锁计算机数据的密钥管理系统。公共密钥基础结构的目的是以安全的方式共享数据。公共密钥基础结构提供计算机和网络应用安全，包括电子商务和网络商务。

详细设计数据（模型、图纸、演示等）、设置权限数据、商家选择数据、竞价和招商数据、财务数据、应急计划、受限的计算机软件等数据项都是内部数据范例。内部数据项必须

根据 NPR1600.1《NASA 安全工程技术规程需求》清晰标记。不能直接标记的数据或数据项，如计算机模型和分析，必须有 NASA 1686 表的复制附件，表明整个数据包都是内部数据。文档要有 NASA 1686 表作为封面。内部文档和数据应被保护。保护内部数据的方式有按需设置的访问权限制、数据复制控制、数据使用时关注、适当的数据标记（文档页眉、页脚、NASA 1686 表）、数据存储在工作室/保险箱内或安全的服务器上、以安全方式传输、按批准的方法销毁（粉碎等）。关于内部数据更多的信息参见 NPR1600.1。

国际武器交易规章执行武器出口控制法案，包括美国军品目录在内。依照武器出口控制法案 38 节和 47 节 7 款，军品目录列出标定为“防御性物品”和“防御性服务”的物品、服务和相关技术数据。国际武器交易规章由美国国务院管理。国际武器交易规章定义的“技术数据”不包括在中学和大学中教授的一般科学、数学或工程原理的信息，不包括公共领域信息（如在 22 CFR120.11 中的定义）^①。它也不包括关于功能、目的或一般系统描述的基本交易信息。为实现国际武器交易规章的目标，需应用如下定义。

- **“军用物品”（22 CFR120.6）：**军用物品是军品目录上的任何物品或技术数据。包括以物理技术状态、模型、样机或者其他方式记录 and 存储的技术数据。

军品目录中的军用物品如下：

- 运载火箭，包括特殊设计或改进的组件、部件、附件、附属装置和相关设备；
- 遥感卫星系统，包括遥测、跟踪和控制卫星的地面控制站，以及使用军品目录中受控的加密单元或上行指令能力的被动地面站；
- 为所有系统特别设计、改进或者配置的组件、部件、附件、附属装置和相关设备（包括地面保障设备）（参见 22 CFR121.1 中的完整列表）。
- **“技术数据”（22 CFR120.10）：**技术数据是用于设计、开发、生产、制造、组装、运行、维修、测试、维护或者改进军用物品的信息。包括以蓝图、图纸、照片、计划、指令和文档形式存在的信息。
- **与军用物品和服务相关的涉密信息：**涉密信息按发明秘密等级确定（35 U.S.C.181 系列；35 CFR 5 卷）。
- **与军用物品直接相关的软件：**受控的软件包括但不限于与军用物品相关的系统功能设计、逻辑流程图、算法、应用程序、操作系统，以及用于设计、实现、测试、运行、诊断和修理的支撑软件。

6.7 技术评估

技术评估是交互关联的流程之一，通过定期技术评审辅助监控工程/项目的技术进展。它还提供状态信息来支持评估系统设计、产品实现和技术管理决策。

6.7.1 流程描述

图 6.7-1 给出技术评估流程的典型流程图，并给出确定技术评估需考虑的典型输入、输出和活动。

^① CFR 是美国联邦条例法典（The Code of Federal Regulations）的缩写，第 22 部的标题为《外交关系》。

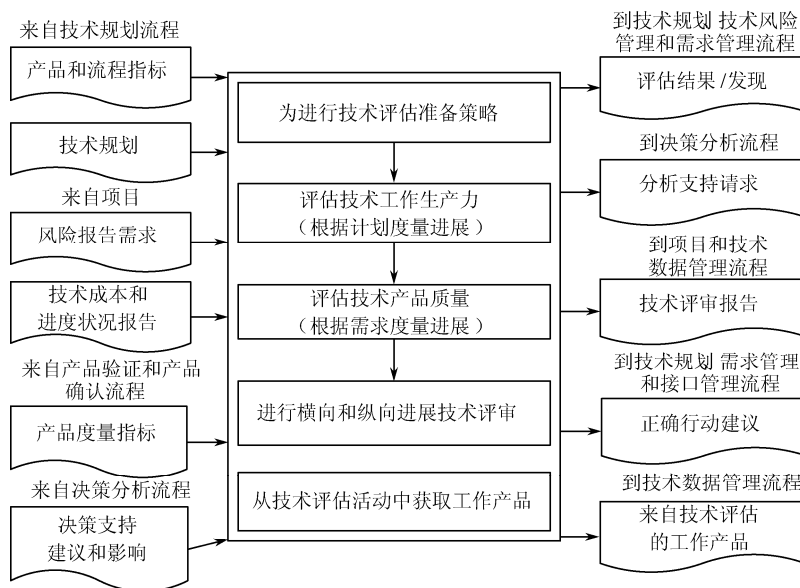


图 6.7-1 技术评估流程

6.7.1.1 输入

技术评估流程需要的典型输入如下所述。

- **技术规划：**这些规划文档描述技术评审/评估流程，同时确定能够决定技术进展的被追踪和评估的技术产品/流程度量指标。这些规划的实例包括系统工程管理计划、评审计划和挣值管理计划。
- **技术指标：**认定为决定技术进展需要追踪的技术指标。这些指标可以表示为效能指标、性能指标和技术性能指标。
- **报告需求：**这些是方法论方面的需求，其中报告关于风险、费用和进度等的技术指标状态。报告状态所用的方法和工具将逐项建立。

6.7.1.2 流程活动

如图 6.7-1 所描述，技术规划（如系统工程管理计划、评审计划）提供技术评估流程的初始输入。这些文档概述技术评审/评估方法，并确定为决定技术进展需追踪和评估的技术指标。技术规划的一个重要部分就是决定在时间、资源和性能方面需要什么来完成满足预期目的和目标的系统。项目负责人需要了解这些计划的进展以便进行适当的管理控制。依据确定技术指标来决定进展的典型活动，包括状态报告和评估数据。状态报告将依据特定的技术指标确认项目实际进展。评估对状态报告的输出进行分析并将其转换为更有用的形式，这样能够决定趋势并理解期望结果的方差。评估活动的结果将传入到决策分析流程（参见 6.8 节），其中可能需要有修正行动。

这些活动一起形成了反馈回路，如图 6.7-2 所示。

这个循环是持续贯穿项目寿命周期的基础。该循环用于项目层次结构的每一层。计划数据、状态报告数据和评估在每一层中适当地分解和集成；决策促使采取的行动逐层向下分解。每一层的负责人决定报告数据和进行评估的频率和形式（与建立在项目结构中更高层的策略保持一致）。在建立这些状态报告和评估需求时，应当遵循的原则如下：

- 使用一致的良好定义的技术指标（参见 6.7.2.2 节）；
- 在所有项目层使用一致的格式报告技术指标；
- 维护历史数据，以确定趋势和进行项目交叉分析；
- 鼓励用逻辑流程积累技术指标（如对项目进展状态使用工作分解结构）；
- 使用定量风险指标支持评估；
- 对所有技术指标使用着色编码（红/黄/绿）提示区域来概要描述项目的条件。

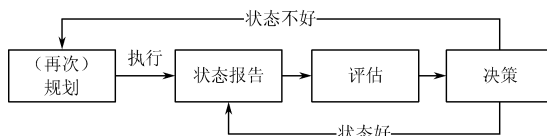


图 6.7-2 规划和状态报告反馈回路

尽管在关注点快速变化或引起新的关注时，某些指标应该更频繁追踪，不过一般推荐规则定期（如每月）的技术指标跟踪。关键评审如初步设计评审和关键设计评审是要点，此时技术指标及其趋势应被仔细评审，以尽早警告潜在问题。一旦发现趋势持续时将产生不利结果，纠正行动应尽可能快地开始。6.7.2.2 节提供了关于成本、进度表（包括挣值管理）、技术性能和系统工程流程指标状态报告和评估技术的更多信息。

在工程和项目技术评审中主要评估技术指标。进行技术评审的典型活动如下：

- 逐阶段地确定、规划和开展技术评审；
- 建立每项评审的目的、目标、启动和成功准则；
- 建立评审小组结构；
- 确定和分解评审导致的行动。

6.7.2.1 节总结了在工程/项目上开展的典型技术评审类型和这些评审支持管理决策流程的作用。该节同时确定了进行评审的一些通用原则，但是没有给出能明确指导工程/项目团队执行评审的定义。

执行技术评估的流程与其他领域，如风险管理、决策分析和技术规划，有密切的关系。这些领域可能为技术评估流程提供输入或者成为该流程输出的受益者。

6.7.1.3 输出

技术评估流程的典型输出如下所述。

- **评估结果、结论和建议：**这里针对已建立指标采集数据，据此可以确定趋势，掌握与期望结果之间的偏差。评估结果将提供给决策分析流程，根据需要决定可能的纠错行动。
- **技术评审报告/记录：**这里收集来自每项评审的信息，获取关于是否满足评审成功准则的结果、建议和行动。

6.7.2 技术评估指南

6.7.2.1 评审、审核和关键决策点

为了能一般地了解根据 NASA 政策（如 NPR7120.5 和 NPR7123.1）召集的各种技术评审，需要检查每个政策文档中的意图。相关评审结果通报给决策机构。NPR7120.5 主要关注的是工程/项目推进到寿命周期下一阶段的准备情况将通报给决策机构。这在每个里程碑评审时完

成，并在整个寿命周期与关键决策点紧密相连。对于关键决策点/里程碑评审，外部独立评审者如独立评审委员会成员，评价工程/项目并最终向决策机构报告其结论。对于准备接受独立评审委员会的工程或项目，技术团队必须实施内部同行评审流程。该流程包括非正式和正式的系统层和子系统层同行评审。本手册试图对前述两个政策文档提供充足的见解和指导，使实践者能够理解如何实现对其成功利用；本手册主要关注内部评审流程。

评审、审核和关键决策点的意图和策略应该在阶段 A 开发，在工程/项目计划中定义。专门执行的这些活动应该与下节中描述的评审和审核类型一致，与 NASA 工程和项目寿命周期图（见图 3.0-1 和图 3.0-2）一致。而评审、审核和关键决策点的时间安排应该适应每个特定项目的需要。

1. 目的和定义

评审的目的是完善机制和流程，为 NASA 管理层和承包商提供如下保证，选择的是最满意的方法、计划或设计；生成的状态控制项满足特定需求，或状态控制项已经准备好。评审帮助促进任务或项目参与者更好地相互理解，打开交流通道，提醒参与者和管理方发现问题并找出解决途径。评审的意图是增加项目的价值，提升项目品质和项目成功的可能。通过邀请外部专家来帮助确定提出的方法、概念和控制基线的可行性，或建议备选方案。评审可能是工程寿命周期阶段评审、项目寿命周期阶段评审或内部评审。

审核的目的是为 NASA 管理层和承包商提供对遵守工程/项目策略、计划、需求和规范的彻底检查。审核是对确定评审活动和相应文档适当性、合理性和有效性的明确证据的系统性检查。审核可能检查政策和流程文档，同时验证对这些政策和文档的遵从度。

设置关键决策点的目的是提供一个预定事件，决策机构决定工程/项目是否已准备好进入寿命周期下一阶段（如从 B 到 C，从 C 到 D 等）或进入下一个关键决策点。关键决策点是 NASA 监管和批准工程/项目流程的组成部分。关于流程和管理监管团队的详细描述，见 NPR7120.5。本质上，关键决策点就像工程和项目必须通过的控制门。在每一阶段，关键决策点之前有一个或多个评审，包括工程管理专家组评审。在每一阶段，允许考虑载人和无人空间飞行工程和项目的差异，但总是以关键决策点结束。关键决策点评审的可能结果如下：

- 批准继续到下一个关键决策点。
- 批准继续到下一个关键决策点，具体行动方案待定。
- 不批准继续到下一个关键决策点。在这种情况下，后续行动包括要求更多信息和进行偏差独立审查；要求进行工程或项目（仅阶段 B、C、D 和 E）的终止评审（见注记）；指明继续执行当前阶段；或工程/项目重新评审。

决策机构评审由工程管理委员会、独立评审委员会、工程负责人、项目负责人和中心管理处提交的材料、协议和工程/项目文档，以支持决策过程。决策机构做出决策需考虑大量因素，包括与 NASA 战略需要、目标和目的连续相关性，NASA 资源的持续费用承受能力，进入下一阶段的可行性和准备状况，剩余的工程或项目（成本、进度、技术和安全方面）的风险。对决策机构最终决定的申诉需提交到更高层的决策机构。

项目终止评审

终止评审由决策机构发起，得出关于是否继续或终止工程或项目的建议。未能保持在控制文档中规定的参数水平将导致考虑终止评审。

在终止评审过程中，工程和项目团队提供相关情况说明，包括所有决策机构要求的材料。需要时，相应支持组织（如采购事物、外部事务、法律事务和公众事务）的代表参加。在最终实施前，决策和决策的依据需要完整归档并由 NASA 主管副局长审查。

2. 项目终止

通常对项目人员来说项目终止是令人失望的,应当注意项目的终止可能是对外部条件改变的适当反应,可能是在对系统效费比的进一步理解基础上的适当反应。

3. 评审的一般原则

某些因素能够影响既定评审的实施计划,如设计复杂性、进度、费用、可视性、NASA 中心实践、评审本身等。因此,在 NASA 中没有制定评审标准,但是,某些关键原理或原则应该包含在评审计划中。包括评审范围、目的、成功准则(与 NPR7123.1 一致)和流程的定义。评审流程的定义应该包括进度鉴别如面对面会谈的时间(议程草案),参与者作用和责任定义,演示资料和数据包内容的确定,以及用做评审内容安排/发出行动请求/评审意见的表格样本。用来筛选和处理差异/请求/意见的评审流程也应包含在计划内。评审之前,评审计划必须经过技术团队领导和项目负责人同意,对于独立评审委员会评审,评审计划须经过独立评审委员会首席同意。

所有评审最好由可用项目需求,以及满足需求的方法、计划或设计的口头汇报组成。这些汇报通常由经认定的设计工程师或其直接指导者提供。同样,除独立评审委员会之外,评审人员最好包括关键利益相关者,如科学团体、工程执行官等。这将确保项目获得能够控制整个项目的人员支持,以及使命任务成功受益人员的支持。邀请与待评审设计不直接相关的项目人员参与(如电力系统人员参与热控系统讨论)是非常有益的。这额外增加了项目利用交叉学科的专业技术发现设计不足或提出改进建议的机会。当然,评审人员也应该包含来自安全、质量和使命任务担保、可靠性、验证和试验领域的非项目专家。

1) 工程寿命周期技术评审

NASA 内部的多种类型工程如下所述。

- **单项目工程**(如“詹姆斯·韦伯”空间望远镜工程^①):趋向于长周期开发和运行使用,表明 NASA 在工程/项目中的大量资源投入,以及来自多个组织和机构对工程/项目的贡献。
- **无耦合工程**(如“发现”工程^②,“空间探索”工程^③):在广泛的科学主题和/或通用工程概念下实施,如为通过商机公示或 NASA 研究通告选定的固定成本项目提供频繁飞行机会。工程中每个项目都独立于其他项目。
- **松耦合工程**(如“火星探测”工程或“无人月球先驱”工程^④):面向特定的科学或探索目标,实施不同范围的多个空间飞行项目。每个单独的项目都设定特定的使命任务目标,在论证流程中开发在架构上和技术上使整体受益的协作和策略。例如,对于所有火星轨道设计寿命超过一年的轨道器,都需要携带支持当前和未来着陆车的通信系统。

① 詹姆斯·韦伯(James Webb)空间望远镜是美国计划中的红外观测太空望远镜,作为即将(原定于 2010 年,现已延长至 2013 年)结束观测活动的哈勃太空望远镜的后续者,计划于 2013 年发射升空。詹姆斯·韦伯(1902-1996)是美国 NASA 的第二任局长,曾领导美国“阿波罗”登月工程等一系列空间探测项目,取得卓越成就。

② “发现”(Discovery)工程是 NASA 空间探索工程的一部分。“发现”工程的目标是发射具有快速研制周期的较小使命任务飞行器,对太阳系进行探测和(或)对太阳系外环境进行遥感探查。

③ “空间探索”(Explorer)工程由 NASA 在 2005 年 9 月发布,其主要内容分为“科学、探测与航宇”和“探测能力”两大部分。其中“科学、探测与航宇”包括科学实验、探测系统和空间飞行三项使命任务。

④ 无人月球先驱工程(Lunar Precursor)是美国为未来载人月球飞行做准备的使命任务。其首次发射的月球勘测轨道飞行器主要目标是为美国人再次登月勘测月球的资源并决定可能的着陆地点。

- **紧耦合工程**（如“星座”工程^①）：拥有多个项目分别执行部分使命任务。单独项目不能实现完整的使命任务。通常，多个 NASA 中心共同为完成工程开展工作。单个项目在不同的中心管理。工程还可能包括其他政府机构或者国际合作者。

所有类型的工程都需要经历表 6.7-1 中列出的两项技术评审。其中主要差异体现在，无耦合/松耦合工程趋向在关键决策点 I 后对其项目进行“状态型”评审，而单项目/紧耦合工程趋向在关键决策点 I 后采用项目寿命周期技术评审流程。

表 6.7-1 工程的技术评审

评 审	目 的
工程/系统需求评审	检查针对工程定义的功能和性能需求（及组成项目），确保需求和选定的构想能满足工程和更高层次的需求。这是一项内部评审。需提供粗略描述的预算和进度表序列
工程/系统定义评审	检查所提议的工程架构及其到系统功能单元的分解过程

在关键决策点 I 之后，单项目/紧耦合工程有必要进行系统级评审。这些评审将项目结合在一起，帮助确保需求分解和系统/子系统整体解决方案满足工程需求。工程级工程评审同样帮助解决项目之间的接口/集成问题。从本手册的观点看，单项目工程和紧耦合工程应遵循下面小节定义的项目寿命周期评审流程。最佳实践和获得的经验表明应驱动工程进行其在项目概念和需求评审之前进行工程的“概念和需求型”评审，并在项目设计和验收评审之后进行工程的“设计和验收型”评审。

2) 项目寿命周期技术评审

多年来，术语“项目寿命周期/里程碑评审”对于不同的 NASA 中心已经含义不同。有些认为它是项目安排的基于被评审项差异和基于预评审的正式评审，其他则认为它表示与行动请求和独立评审委员会/关键决策点流程密切相关的活动。本文使用后者定义该术语。项目寿命周期评审是决策机构召集的强制性评审，将贯穿项目寿命周期的内部技术流程（同行评审）结果提供给 NASA 管理团队和独立审查专业小组，如独立评审委员会（见 NPR7120.5）。这些评审用于评估项目的进展和状况，向 NASA 保证选定的是最满意方法、计划或设计，且生成的状态控制项满足特定需求或状态控制项可以发布和使用。寿命周期评审的例子包括系统需求评审、初步设计评审、关键设计评审和验收评审。

指定的寿命周期评审之后紧接着是一个关键决策点，项目决策机构基于寿命周期评审小组的结果和建议，决定项目是否进入寿命周期下一个阶段。

3) 独立评审委员会

独立评审委员会的作用是向工程/项目及召集机构提供咨询，无权管理工程/项目的任何内容。委员会针对技术性方法和工程性方法、风险态势进行评审，并根据工程/项目控制基线进展提供专家评估意见。适当时，它可以提出提高性能或降低风险的建议。

4) 内部评审

在项目或任务过程中，有必要进行内部评审，向同行评价与评论小组提供技术途径、权衡研究、分析和问题领域。评审的时间安排、参与者和内容通常由项目负责人或评审组织管理者在技术团队的辅助下确定。在准备寿命周期评审时，项目启动其项目计划中定义的内部

① “星座”（Constellation）工程是美国 NASA 正在筹备的空间探索计划，整个工程包括一系列新的航天飞行器、运载火箭和相关设施，将在包括国际空间站补给，以及登月等各种空间使命任务中使用。预定的首次发射日期是 2015 年 3 月。

评审流程。这些评审不仅是交换思想和解决问题的会议，还允许通过评审技术途径、权衡研究和分析，建立项目需求、计划和设计控制基线的内部评审。

内部同行评审为控制项目技术进展提供了一个极好的方法。这些评审也应用于确保所有关注团体在流程早期进入并在整个流程中参与开发。因此，来自如制造和质量保证领域的代表应作为主动参与者参加内部评审。来自为待评审系统或子系统提供支持、开发与其相接的系统或子系统的其他中心和外部组织的代表参与评审同样是好的做法。这样做能够确保设计是可生产和可集成的，确保在项目寿命周期内的质量管理。

由于内部同行评审比寿命周期评审更加详细，审查小组可以利用内部和外部的专家帮助开发和评估内部审查的方法和概念。某些组织内组建“红队”提供内部的、独立的同行审查，确定不足和提出建议。项目通常称其内部评审是“桌面”评审或“中期”设计评审。无论怎样命名，目的都相同，即确保项目寿命周期评审成功的控制基线准备就绪。

值得一提的是，由于这些评审的重要性，每项评审应该在评审之前有良好定义的启动和成功准则。

4. 必要的技术评审

本小节描述 NPR7123.1 要求的 NASA 工程和项目寿命周期内技术评审的目的、时序、目标、成功准则和结果。意图是为工程/项目负责人和系统工程师提供指导信息，同时表明评审活动和系统工程产品逐渐成熟的过程。对于飞行系统和地面保障项目，NASA 寿命周期的规划论证和实施执行阶段分成 7 个项目阶段。下列清单帮助准备特定的评审启动和成功准则，但并非替代它们。为使额外工作最小化，评审材料应该是工程/项目的关键文档。

1) 工程/系统需求评审

工程/系统需求评审用于确保工程需求论证是合适的，与 NASA 和使命任务主管的战略目标相关联。评审的启动准则和成功准则见表 6.7-2。

表 6.7-2 工程/系统需求评审启动和成功准则

工程/系统需求评审	
启动准则	成功准则
(1) 规划论证授权文档已经被批准。 (2) 工程需求已经定义，支持该工程的使命任务主管需求。 (3) 主要工程风险已经识别，相应的缓解策略已经确定。 (4) 工程的高层需求已经归档，其内容如下： <ul style="list-style-type: none"> • 性能需求； • 安全需求； • 工程性需求。 (5) 验证是否服从工程需求的方法已经定义。 (6) 控制工程需求变更的技术规程已经定义并获得批准。 (7) 单独项目的工程需求可追踪性已经根据如 NASA 战略规划中所描述的 NASA 需要、目的和目标归档。 (8) 对技术、安全、成本和进度有显著影响的工程/项目顶层风险已经识别	(1) 针对使命任务和科学需求定义的高层工程需求已经确定并被批准。 (2) 定义的与其他工程接口已获批准。 (3) 为提供具有高成本效益的工程，工程需求已经确定。 (4) 工程需求被单项目工程或工程的多个项目适当地采用。 (5) 控制工程需求变更的计划已被批准。 (6) 验证满足工程需求的方法已被批准。 (7) 处理已识别主要风险的缓解策略已被批准

2) 工程/系统定义评审

工程/系统定义评审应用到所有的 NASA 空间飞行工程, 确保这些工程能够实施已批准的工程议定协议。批准的工程议定协议允许工程从规划论证阶段转移到实施执行阶段。工程审批准评审作为工程/系统定义评审的一部分进行, 对工程进入实施执行阶段准备情况的独立评估应向 NASA 总局管理层提交报告。

工程/系统定义评审检查所提议的工程架构和系统功能单元的分解流程。对提议的工程目标和满足这些目标的概念进行评价; 辨识和评估关键技术和其他风险; 提出工程计划、预算和进度表的控制基线。技术团队提供支撑工程/系统定义评审的技术内容。评审的启动准则和成功准则见表 6.7-3。

表 6.7-3 工程/系统定义评审启动和成功准则

工程/系统定义评审	
启动 准 则	成 功 准 则
<p>(1) 工程/系统需求评审已经满意地完成。</p> <p>(2) 工程计划已经准备就绪, 包括下列内容:</p> <ul style="list-style-type: none"> • 工程如何管理; • 特定项目列表; • 高层工程需求 (包括风险准则); • 与 NASA 总局和主管部门的战略目标相关的性能、安全性、工程性需求; • 待开发系统 (硬件和软件) 描述, 包括已有系统、系统接口和设施; • 影响系统开发的主要约束鉴别 (如成本、发射窗口、需要的运载火箭、使命任务空间飞行环境、引擎设计、国际合作者和技术动因)。 <p>(3) 工程层系统工程管理工作计划, 包括项目技术方法和管理计划, 用于实现分配的工程需求, 如发射、飞行和地面系统, 以及使用和后勤保障构想。</p> <p>(4) 独立成本分析和独立成本估算。</p> <p>(5) 预算外的资源管理工作计划。</p> <p>(6) 制定工程议定协议的文档, 包括以下内容:</p> <ul style="list-style-type: none"> • 工程使命任务解决方案的可行性, 包括可接受费用范围内的成本估算; • 适合项目初始论证阶段的项目规划; • 用于项目评价的工程概念评价准则的确定和优先排序; • 估算需要的年度经费水平; • 可靠的工程成本和进度表到每个项目的分配估计; • 可接受的风险和缓解策略 (由技术风险评估支持); • 组织结构和已定义的工作安排; • 已定义的工程采办策略; • 与其他工程和合作伙伴的接口; • 工程实施计划草案; • 已定义的工程管理系统。 <p>(7) 工程控制计划草案, 包括的内容如下:</p> <ul style="list-style-type: none"> • 工程计划对工程需求、技术设计、进度表和成本的控制能否达到高层需求; • 工程需求、技术设计、进度表和成本如何控制; • 工程如何利用其技术、进度表和成本储量来控制基线; • 工程计划如何向使命任务主管助理报告技术、进度表和成本状态, 包括报告频率和详细程度; • 工程如何解决技术免责声明和如何处理不同的观点。 <p>(8) 对于每一个项目, 顶层描述已经归档</p>	<p>(1) 工程计划和管理方法已获批准。</p> <p>(2) 系统工程管理计划和技术方法已获批准。</p> <p>(3) 估算成本是适当的。</p> <p>(4) 制定的工程议定协议文档被批准。</p> <p>(5) 工程控制计划草案已获批准。</p> <p>(6) 达成工程能够支持 NASA 总局需求、目的和目标的协议。</p> <p>(7) 技术方法是适当的。</p> <p>(8) 进度表是适当的, 并且与成本、风险和使命任务目标一致。</p> <p>(9) 预算外资源是适当的和可用的</p>

3) 使命任务概念评审

使命任务概念评审证实使命任务需求并检查提出的使命任务目标和达到这些目标的构想。这是通常发生在系统开发认定组织的内部审查。使命任务概念评审应在进入概念开发阶段（阶段 A）之前完成。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-4。
- 确保评审中发现的问题适当归档和准备好解决方案计划。

评审结果

成功的使命任务概念评审支持如下决定，提出的使命任务满足客户需要，并有充分的质量和值支持外场中心管理决策，向 NASA 工程主管副局长提出阶段 A 的进一步研究工作。

表 6.7-4 使命任务概念评审启动和成功准则

使命任务概念评审	
启动准则	成功准则
(1) 使命任务目标和目的。 (2) 分析备选的概念，并表明至少有一个可行。 (3) 运行使用构想。 (4) 初步的使命任务溢出范围选项。 (5) 初步风险评估，包括技术风险和 Related 风险管理/缓解的策略和选项。 (6) 概念试验和评价策略。 (7) 到达下一阶段的初步技术计划。 (8) 已定义的效能指标和性能指标。 (9) 概念化寿命周期保障策略（后勤保障，生产制造，运行使用等）	(1) 使命任务目标清晰地定义和声明，并且是明确的和内部一致的。 (2) 初始的需求集满意地提供给系统，使之满足使命任务目标。 (3) 使命任务可行。解决方案已经确定，并且技术上可行。大致的成本估算在可接受的费用范围内。 (4) 待评价系统所用的概念评价准则已经确定，并已按优先级排序。 (5) 使命任务的需要已经清晰地确定。 (6) 成本和进度估算是可信的。 (7) 完成技术搜索更新，确定已有的满足使命任务或部分使命任务的资产或产品。 (8) 技术计划充分，可进入下一阶段。 (9) 风险和缓解策略已经确定，并且根据技术评估是可接受的

4) 系统需求评审

系统需求评审检查为系统和初步工程或项目计划定义的功能和性能需求，确保需求和选定的概念满足使命任务。系统需求评审在概念开发阶段（阶段 A）进行系统定义评审或使命任务概念评审之前进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-5。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

成功完成的系统需求评审将固化工程/项目需求，据此，负责工程的 NASA 主管副局长做出正式决策，继续进行提议的项目实施的必要准备工作。

表 6.7-5 系统需求评审启动和成功准则

系统需求评审	
启动准则	成功准则
<p>(1) 使命任务概念评审的成功完成和对所有使命任务概念评审的行动请求和评审内容偏差作出响应。</p> <p>(2) 初步系统需求评审议程、成功准则、委员会职责在系统需求评审之前已经过技术团队、项目负责人和评审首席同意。</p> <p>(3) 下列硬件和软件系统单元的技术产品，在评审前可提供给认定的参与者：</p> <ul style="list-style-type: none">• 系统需求文档；• 系统软件功能性描述；• 更新后的运行使用构想；• 如果存在，更新后的使命任务需求；• 控制基线确定的系统工程管理计划；• 风险管理计划；• 系统需求到较低层系统的初步分配；• 更新后的成本估算；• 技术开发成熟度评估计划；• 更新后的风险评估和缓解方法（可能时，包括概率风险评估）；• 后勤保障文档（如初步维护计划）；• 可能时，初步员工评估计划；• 软件开发计划；• 系统安全与使命任务担保计划；• 技术状态管理计划；• 初始文档目录；• 验证和确认方法；• 初步系统安全性分析；• 需要时，其他专业学科要求	<p>(1) 项目利用可靠的流程在所有层次分配和控制需求，在进度约束下完成需求定义活动的计划制定。</p> <p>(2) 完成与顶层使命任务和科学需求相关的需求定义，完成与外部实体和主要内部单元之间的接口定义。</p> <p>(3) 完成定义针对子系统层的关键主导需求的分配和分解。</p> <p>(4) 确定直到子系统层的如何验证和确认需求的初步方法。</p> <p>(5) 完成辨识主要风险并已进行技术评估，完成可行的缓解策略定义</p>

5) 使命任务定义评审（仅针对无人飞行）

使命任务定义评审检查提出的需求、使命任务架构和使命任务到所有功能单元的分解，确保全局概念是完整的、可行的，且与可用资源一致。

使命任务定义评审在概念探索阶段（A 前阶段）完成后和初步设计阶段（阶段 B）之前的概念研究与技术开发阶段（阶段 A）进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动法则和成功法则见表 6.7-6。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

成功的使命任务定义评审支持针对进一步开发系统架构/设计和任何完成使命任务所需技术的决策。该结果增强使命任务的价值，为系统采办策略提供基础。

表 6.7-6 使命任务定义评审启动和成功准则

使命任务定义评审	
启动 准 则	成 功 准 则
<p>(1) 系统需求评审的成功完成和对系统需求评审所有行动请求和评审内容偏差作出响应。</p> <p>(2) 初步使命任务定义评审议程、成功准则、委员会职责在使命任务定义评审之前已经过技术团队、项目负责人和评审首席同意。</p> <p>(3) 下述硬件和软件系统单元的技术产品，在评审前可提供给认定参与者：</p> <ul style="list-style-type: none">• 系统架构；• 更新后的系统需求文档，如果有；• 系统软件功能性描述；• 更新后的运行使用构想，如果有；• 更新后的使命任务需求，如果有；• 更新后的系统工程管理计划，如果有；• 更新后的风险管理计划，如果有；• 技术开发成熟度评估计划；• 偏好的系统解决方案定义，包括主要的权衡和选项；• 更新后的风险评估和缓解方法（包括概率风险评估，如果可能）；• 更新后的成本和进度数据；• 后勤保障文档（如初步维护计划）；• 软件开发计划；• 系统安全与使命任务担保计划；• 技术状态管理计划；• 更新后的初始文档目录，如果有；• 初步系统安全性分析；• 其他需要的特殊专业	<p>(1) 作为结果的所有构想是合理的、可行的、完整的，是对使命任务需求的响应，与系统需求和可用资源（成本、进度、质量和能源）一致。</p> <p>(2) 系统和子系统设计方法和运行使用构想已经形成，并与需求集保持一致。</p> <p>(3) 需求、设计方法和概念设计将在估算的成本内完成使命任务需要。</p> <p>(4) 主要风险已经辨识并经过技术评估，可行的缓解策略已经定义</p>

6) 系统定义评审（仅限于载人空间飞行）

系统定义评审检查提出的系统架构/设计和系统到所有功能单元的分解。系统定义评审在概念开发阶段（阶段 A）结束和初步设计阶段（阶段 B）开始前进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-7。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为系统定义评审成功完成的结果，系统及其运行使用被很好的理解，从而保证最终成品的设计和采办。已批准的系统及其部段的规范，适当功能单元设计的初步规范可以发布。已经建立技术状态管理计划，用来控制设计和需求变更。控制和集成扩展技术流程的计划已经就绪。

表 6.7-7 系统定义评审启动和成功准则

系统定义评审	
启动准则	成功准则
<p>(1) 系统需求评审成功完成和对系统需求评审所有行动请求和评审内容偏差作出响应。</p> <p>(2) 初步系统定义评审议程、成功准则、委员会职责在系统定义评审之前已获技术团队、项目负责人和评审首席同意。</p> <p>(3) 下述硬件和软件系统单元系统定义评审技术产品，在评审前可提供给认定参与者：</p> <ul style="list-style-type: none">• 系统架构；• 首选的系统解决方案定义，包括主要的权衡和选项；• 更新后的控制基线文档，根据需要；• 初步功能控制基线（支持权衡分析和数据）；• 初步系统软件功能需求；• 系统工程管理计划变更，如果有；• 更新后的风险管理计划；• 更新后的风险评估和缓解方法（包括概率风险评审，如果有）；• 更新后的技术开发成熟度评估计划；• 更新后的成本和进度表数据；• 更新后的后勤保障文档；• 基于系统复杂度，更新的人员定级计划；• 软件测试计划；• 软件需求文档；• 接口需求文档（包括软件）；• 技术资源利用评估和余量；• 更新后的系统安全与使命任务担保计划；• 更新后的初步安全性分析	<p>(1) 完成定义系统需求，包括使命任务成功准则和投资方强加的所有约束，并且形成提出概念设计的基础。</p> <p>(2) 所有技术需求已分配，且到子系统的分解是适当的。需求、设计方法和概念设计能够根据可用的资源（成本、进度、质量和能源）完成使命任务需要。</p> <p>(3) 需求流程是可靠的，能合理期望其以实时的开发方式持续确定和分解细化需求。</p> <p>(4) 技术方法是可信的并且可对确定需求做出的响应。</p> <p>(5) 技术计划已经在需要时更新。</p> <p>(6) 权衡已经完成，为阶段 B 计划的权衡适当地考虑选择空间。</p> <p>(7) 开发、使命任务和安全方面的重大风险已确定并经过技术评估，且已有管理风险的流程和资源。</p> <p>(8) 针对任何新的辅助技术开发，已有适当的计划。</p> <p>(9) 运行使用构想与提出的设计构思一致，并且符合使命任务需求</p>

7) 初步设计评审

初步设计评审验证初始设计在可接受的风险范围，以及成本和进度约束之内满足系统所有需求，并为进行详细设计建立基础。它表明已经选定正确的设计选项，已经确定系统接口，已经创建接近 10%的工程技术图纸，已经说明验证方法。初步设计评审在初步设计阶段（阶段 B）接近完成时作为规划论证阶段的最后一次评审进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-8。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为初步设计评审成功完成的结果，产品设计控制基线得到批准。成功评审结果还授权项目进入到实施和详细设计阶段。

表 6.7-8 初步设计评审启动和成功准则

初步设计评审	
启动 准 则	成 功 准 则
<p>(1) 系统定义评审或使命任务定义评审成功完成，并对系统定义评审或使命任务定义评审所有行动请求和评审内容偏差作出响应，或对所有仍然进行的评审已形成适时的终止计划。</p> <p>(2) 初步设计评审议程、成功准则、委员会职责在评审之前已经过技术团队、项目负责人和评审首席同意。</p> <p>(3) 下述硬件和软件系统单元的初步设计评审技术产品，在评审前可提供给认定的参与者：</p> <ul style="list-style-type: none">• 需要时，更新后的控制基线文档。• 需要时，每一个状态控制项（包括硬件和软件）的初步子系统设计规范支持权衡分析和数据。初步软件设计规范应包括软件架构的完整定义和可用的初步数据库设计描述。• 更新后的技术开发成熟度评估计划。• 更新后的风险评估和缓解方法。• 更新后的成本和进度表数据。• 需要时，更新后的后勤保障文档。• 可用的技术规划（如技术性能度量计划，污染控制计划，部件管理计划，环境控制计划，电磁干扰/电磁兼容性控制计划，载荷到运载集成计划，可生产性/制造能力工程计划，可靠性工程计划，质量保证计划）。• 可用标准。• 安全性分析和计划。• 工程技术草图目录。• 接口控制文档。• 验证和确认计划。• 需要时，对规章（如国家环境政策法案）要求的响应计划。• 处置计划。• 技术资源利用估算和余量。• 系统级安全性分析。• 初步有限寿命产品清单	<p>(1) 顶层需求，包括使命任务成功准则，技术性能指标，任何投资方强加的约束意见都一致，最终定案，清晰陈述，并与初步设计保持一致。</p> <p>(2) 可验证的需求分解是完整的和适当的；如果不是，则已对进行中的工作制定适时解决方案的适当计划。需求对使命任务目标和目的是可追踪的。</p> <p>(3) 初步设计有望在可接受的风险水平上满足需求。</p> <p>(4) 技术接口的定义与整体技术成熟度保持一致，并且风险水平是可接受的。</p> <p>(5) 适当的技术接口与整体技术成熟度保持一致，并且风险水平是可接受的。</p> <p>(6) 技术性能指标存在适当的技术余量。</p> <p>(7) 任何需要的新技术已经开发到适当的可用状态，或存在备份选项且拥有使其成为可用技术的保障能力。</p> <p>(8) 项目风险已经得到了了解，且进行了可靠的评估，已确定有效管理风险的计划、流程和资源。</p> <p>(9) 安全与使命任务担保（如安全性、可靠性、可维修性、质量和电子电气和机电部件）已经在初步设计中适当考虑，任何可用的安全与使命任务担保产品（如概率风险评估、系统安全性分析、失效模式和影响分析）已经得到批准。</p> <p>(10) 运行使用构想技术上可行，包括（适当的）人为因素，包括执行运行使用构想的需求分解</p>

8) 关键设计评审

关键设计评审的目的是，验证设计成熟度足以支持进行全尺寸制造、组装、集成和试验，技术工作可以正常完成飞行和地面系统开发，以及使命任务应用，以在确定的成本和进度约束下满足使命任务性能需求。大约 90%的工程技术图纸得到批准并发布进行制造。关键设计评审在详细设计阶段（阶段 C）进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-9。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为关键设计评审成功完成的结果，待建造产品的控制基线、生产和验证计划已获批准。

成功的评审结果还（根据提交评审的待建产品控制基线和编码标准）授权交付软件编码、系统合格试验和集成。所有未决问题应该由终止行动和计划来解决。

表 6.7-9 关键设计评审启动和成功准则

关键设计评审	
启动准则	成功准则
<p>(1) 初步设计评审的成功完成和对初步设计评审所有行动请求和评审内容偏差作出响应，或者对所有仍然进行的评审已形成适时完成计划。</p> <p>(2) 初步的关键设计评审议程、成功准则、委员会职责在关键设计评审之前已经过技术团队、项目负责人和评审首席同意。</p> <p>(3) 下述硬件和软件系统单元的关键设计评审需要的技术工作产品，在评审前可提供给认定的参与者：</p> <ul style="list-style-type: none"> • 需要时，更新后的控制基线文档； • 每个硬件和软件状态控制项的产品待建规范，同时支持权衡分析和数据； • 制造、组装、集成和试验计划和技术规程； • 技术数据包（如集成图表、备件供应清单、接口控制文档、工程技术分析和规范）； • 运行使用限制和约束； • 技术资源效用估算和余量； • 验收标准； • 指令和遥测数据列表； • 验证计划（包括需求和规范）； • 确认计划； • 发射场运行使用计划； • 检查和启用计划； • 处置计划（包括退役或终止）； • 更新后的技术开发成熟度评估计划； • 更新后的风险评估和缓解； • 更新后可靠性分析和评估； • 更新后的成本和进度表数据； • 更新后的后勤保障文档； • 软件设计文档（包括接口设计文档）； • 更新后的有限寿命产品清单； • 子系统级和初步运行使用安全性分析； • 系统和子系统认证计划和需求（需要时）； • 与验证相关的系统安全性分析 	<p>(1) 详细设计有望在可接受的风险水平上和适当的余量下满足需求。</p> <p>(2) 接口控制文档充分成熟可进行制造、组装、集成和试验，并且已制定涉及外部的产品管理计划。</p> <p>(3) 对产品控制基线确定有高度信心，已有或将有充足的文档以适时的方式允许推进制造、组装、集成和试验过程。</p> <p>(4) 产品验证和产品确认的需求和计划是完整的。</p> <p>(5) 试验方法是全面的，系统组装、集成、试验，以及发射场和使命任务运行的计划是充分的，可以进入下一阶段。</p> <p>(6) 存在足够的技术性和工程性余量和资源，保证在预算、进度和风险约束范围内完成开发。</p> <p>(7) 使命任务成功的风险已被了解并经历可信的评估，存在有效地管理风险的计划和资源。</p> <p>(8) 安全与使命任务担保（如安全性、可靠性、维修性、质量和电子电气及机电部件）在系统设计和运行使用设计时已经得到充分考虑，任何可用的安全与使命任务担保计划产品（如概率风险评估、系统安全性分析、失效模式和影响分析）已经得到批准</p>

9) 生产准备状态评审

生产准备状态评审在飞行系统和地面保障项目开发时或需获取由项目决定的多个（大于三个）相似系统时进行。生产准备状态评审确定系统开发人员有效地生产所需数量系统的准备情况。生产准备状态评审确保生产计划，制造、组装和集成的辅助产品准备就绪，以及人员就位并且准备开始生产。生产准备状态评审在详细设计阶段（阶段 C）进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功法则见表 6.7-10。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为生产准备状态评审成功完成的结果，用于最终生产的待建产品控制基线、生产和验证计划获得批准。图纸获准发布和授权生产。成功的评审结果还（根据评审中提交的待建产品控制基线和编码标准）授权可交付软件编码、系统合格试验和集成。所有未决问题应该由终止行动和计划来解决。

表 6.7-10 生产准备状态评审启动和成功准则

生产准备状态评审	
启动准则	成功准则
(1) 在开发阶段遇到的重大生产工程技术问题得到解决。 (2) 设计文档足够支持生产。 (3) 生产计划和准备足以开始制造。 (4) 辅助生产的产品和充足的资源可用，已经分配，并可支持目标产品的生产	(1) 设计已经得到充分的认证。 (2) 系统需求在最终生产技术状态中能够完全满足。 (3) 已经准备好适当的措施支持生产。 (4) 面向制造的设计考虑确保生产和组装的灵活和高效。 (5) 风险已经识别并进行可信的评估和特征化，缓解工作已经定义。 (6) 材料清单已经评审，关键部件得到确认。 (7) 交付进度表已经验证。 (8) 资源的备选来源已经适当确定。 (9) 充分的备件已经做好计划和预算。 (10) 需要的设施和工具对于目标产品的生产是充分的。 (11) 指定的特殊工具和试验设备数量适当可用。 (12) 生产和保障人员是合格的。 (13) 图纸已经过认证。 (14) 生产工程技术和计划对于高效益生产足够成熟。 (15) 生产流程和方法与质量需求保持一致，适应职业安全、环境规则和能量守恒定律。 (16) 对于需采购的原材料有合格的供应商

10) 系统集成评审

系统集成评审确保系统已做好集成准备。部段、组件和子系统可用并且已经准备好集成到系统中。集成设施、保障人员、集成计划和技术规程已为集成做好准备。系统集成评审在详细设计阶段（阶段 C）结束和系统组装、集成和试验阶段（阶段 D）开始前进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功法则见表 6.7-11。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为系统集成评审成功完成的结果，最终已建产品的控制基线和验证计划获得批准。图纸获准发布并授权支持集成。所有未决问题应该由终止行动和计划来解决。已经为子系统/系统集成技术规程，包括地面保障设备、设施，后勤需求和保障人员做出计划并为保障集成做好准备。

11) 试验准备状态评审

试验准备状态评审确保试验件（硬件/软件）、试验设施、保障人员和试验技术规程已经准备好试验及数据获取、简化和控制。试验准备状态评审在验证或确认试验开始前进行。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-12。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

成功的试验准备状态评审意味着试验与安全工程师证明准备工作已经完成，项目负责人授权正式试验开始。

表 6.7-11 系统集成评审启动和成功准则

系统集成评审	
启动 准 则	成 功 准 则
(1) 集成计划和技术规程已经完成并获得批准。 (2) 部和组件可供集成使用。 (3) 机械和电子接口已经根据接口控制文档得到验证。 (4) 所有可用的功能性试验、元件及子系统试验、合格试验已经成功进行。 (5) 集成设施，包括无尘房间、地面保障设备、紧固操作设备、高架起重机、电子测试设备已准备就绪并且可用。 (6) 保障人员已经完成适当培训。 (7) 操控和安全性需求已经归档。 (8) 所有已知的系统差异已经识别，根据审批的计划得到处理。 (9) 所有前期设计评审成功准则和关键内容根据审批的计划已经得到满足。 (10) 质量控制组织已经做好准备支持集成工作	(1) 待集成系统的相应集成计划和技术规程已经完成并获得批准。 (2) 前期的组件、子系统和系统试验结果为进行集成形成满意的基准。 (3) 需要时，风险水平已经辨识并被工程/项目领导层接受。 (4) 集成技术规程和工作流程已经清晰地定义和归档。 (5) 集成计划、集成技术规程和环境的评审，以及待集成产品的技术状态评审，为合理期望集成成功提供保证。 (6) 集成人员已经在集成和安全技术规程方面接受充分的培训

表 6.7-12 试验准备状态评审启动和成功准则

试验准备状态评审	
启动 准 则	成 功 准 则
(1) 试验目标已清晰定义和归档，所有试验计划、技术规程、环境、试验件的技术状态支持这些目标。 (2) 试验条件下的系统技术状态已经定义且获得认可。评审之前，所有的接口已经根据技术状态管理准备就绪，或根据议定的计划完成定义，并且版本描述文档可供试验准备状态评审参与者使用。 (3) 所有可用的功能性、元件级、子系统、系统和合格试验已经成功进行。 (4) 所有试验准备状态评审指定的材料，如试验计划、试验大纲和技术规程，在进行评审前能够供所有的参与者使用。 (5) 所有已知的系统差异已经确定，根据审批的计划得到处理。 (6) 所有前期设计评审成功准则和关键内容根据审批的计划已经得到满足。 (7) 所有需要的试验资源如人员（包括指定的试验负责人）、设施、试验件、试验仪器和其他辅助产品已经确定，可以支持需要的试验。 (8) 所有试验参与者的作用和职责已经明确并且获得认可。 (9) 试验意外应急计划已经完成，所有人员已经得到培训	(1) 对试验条件下的系统，适当的试验计划已经完成并得到批准。 (2) 所需试验资源的相应鉴别和协调已经完成。 (3) 前期组件、子系统和系统试验结果为进行计划的试验提供满意的基准。 (4) 需要时，风险水平已经确定，并且被工程或相关领导层接受。 (5) 从试验项目中获取经验教训的计划已经归档。 (6) 试验的目标已经清晰定义和归档，所有试验计划、技术规程、环境和试验件技术状态的评审，提供目标能够满足的合理期望。 (7) 试验大纲的期望结果已经评审和分析，结果与试验计划 and 目标是一致的。 (8) 在试验运行和安全技术规程方面，试验人员已接受适当培训

12) 系统验收评审

系统验收评审验证目标产品与其预期成熟度水平相关的完整性，评估与利益相关者期望的相符程度。系统验收评审检查系统、目标产品和文档，以及支持验证的试验数据和分析。系统验收评审同样确保系统已有足够的技术成熟度，可授权运送到指定的运行使用设施或发射场。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-13。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为系统验收评审成功完成的结果，系统已经被买方接受，已得到授权运送硬件到发射场或运行使用设施，可为运行使用安装软件和硬件。

表 6.7-13 系统验收评审启动和成功准则

系统验收评审	
启动 准 则	成 功 准 则
(1) 在系统验收评审之前，（正常）完成初步议程协调。 (2) 下列系统验收评审技术产品在评审前可供认定参与者使用： <ul style="list-style-type: none">• 主要供应商进行系统验收评审的结果；• 交付生产或制造的计划；• 产品验证结果；• 产品确认结果；• 说明可交付系统符合已建验收标准的文档；• 说明系统在期望的运行使用环境中工作正常的文档；• 更新后的技术数据包，包括所有试验结果；• 认证数据包；• 更新后的风险评估和缓解方法；• 成功完成的前期里程碑评审；• 对终止评审保留的处置权和继续评审的行动和计划	(1) 需要的试验和分析是完整的，表明系统在期望的运行环境中是正常的。 (2) 风险已知并且可控。 (3) 系统满足设定的验收标准。 (4) 所需的安全运输、处理、检查和运行使用计划和技术规程是完整的且可使用的。 (5) 技术数据包是完整的，反映所交付的系统。 (6) 已总结获得对组织改进和系统运行使用有益的经验教训

13) 运行使用准备状态评审

运行使用准备状态评审检查实际系统的特性和用于系统或目标产品运行使用的技术规程，确保所有的系统和（飞行和地面）保障硬件、软件、人员、技术规程和用户文档准确反映系统的部署状态。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动和成功准则见表 6.7-14。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为运行使用准备状态评审成功完成的结果，系统已经准备好承担正式运行使用。

表 6.7-14 运行使用准备状态评审启动和成功准则

运行使用准备状态评审	
启动准则	成功准则
<p>(1) 所有确认试验已经完成。</p> <p>(2) 确认试验中的不足和异常已经得到解决，结果已并入到所有运行使用保障和辅助产品中。</p> <p>(3) 所有正常和应急的运行使用保障和辅助产品（如设施、设备、文档、更新后的数据库）已经试验，并且分发/安装到需要支持运行使用的场站。</p> <p>(4) 运行使用手册已经获得批准。</p> <p>(5) 已经为用户和操作人员提供正确运行使用系统技术规程的培训。</p> <p>(6) 运行使用应急计划已经完成，且所有人员已接受培训</p>	<p>(1) 系统，包括任何辅助产品，已经确定为系统运行使用状态准备就绪。</p> <p>(2) 已获得对改进组织管理和系统运行使用有益的所有经验教训。</p> <p>(3) 所有免责声明和变更声明已经处理完毕。</p> <p>(4) 系统硬件、软件、人员和技术规程已经准备好支持运行使用</p>

14) 飞行准备状态评审（见表 6.1-15）

飞行准备状态评审检查那些决定系统已经为安全和成功飞行或发射，以及后续飞行准备就绪的试验、演示、分析和审核。飞行准备状态评审确保所有的飞行和地面硬件、软件、人员和技术规程已为运行使用准备就绪。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-15。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

评审结果

作为飞行准备情况评审成功完成的结果，技术和技术规程成熟度达到系统发射和飞行授权及某些情况下开始运行使用要求。

表 6.7-15 飞行准备状态评审启动和成功准则

飞行准备状态评审	
启动准则	成功准则
<p>(1) 得到飞行运行在可接受的风险下能够安全进行的证明。</p> <p>(2)系统和保障单元确定处于适当技术状态并做好飞行准备。</p> <p>(3) 接口兼容，且发挥预期功能。</p> <p>(4) 基于“通过”或“不通过”准则，系统状态支持“通过”发射决策。</p> <p>(5) 来自前期完成的飞行和评审中的飞行失效问题和异常已经得到解决，结果已经并入到所有运行使用的保障和辅助产品中。</p> <p>(6) 系统已经进入飞行技术状态</p>	<p>(1) 飞行器已做好飞行准备。</p> <p>(2) 硬件适合于可信的安全飞行（即满足已建立的可接受风险标准或被工程负责人和指定管理机构接受并归档）。</p> <p>(3) 飞行和地面软件单元已经做好保障飞行和飞行运行准备。</p> <p>(4) 接口已检查并且功能正常。</p> <p>(5) 未决的事项和免责声明已经检查并且是可接受的。</p> <p>(6) 飞行和返回环境因素符合约束范围。</p> <p>(7) 所有未决的安全性和使命任务风险事项已经处理</p>

15) 发射后评估评审

发射后评估评审是空间飞行器系统部署后对进入全面常规运行使用准备状态的评价。评审根据发射后飞行运行经历评价项目的状态、性能和能力。这也意味对准备状态评估的责任从开发组织转移到运行组织。该评审同时评价项目计划的状态和执行使命任务的能力，重点在于近期运行使用和使命任务的关键事件。评审通常在早期飞行运行和初始检查之后进行。

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-16。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

表 6.7-16 发射后评估评审启动和成功准则

发射后评估评审	
启动 准 则	成 功 准 则
<p>(1) 能够获得发射和早期运行的性能，（可能时）包括早期推进机动的结果。</p> <p>(2) 能够获得观测到的空间飞行器和科学仪器性能，包括仪器校准计划和状态。</p> <p>(3) 运载火箭性能评估和使命任务圆满完成，包括发射事件序列评估和获取发射运行中的经验教训。</p> <p>(4) 能够获得使命任务运行和地面数据系统经验，包括追踪和数据获取保障及空间飞行器遥测数据分析。</p> <p>(5) 能够获得使命任务运行组织，包括职员、设施、工具和任务软件（如空间飞行器分析等）的状态。</p> <p>(6) 飞行异常和采取的响应行动都已归档，包括空间飞行器采取的自动故障保护行动，或任何无法解释的空间飞行器遥测数据，如警报。</p> <p>(7) 技术规程、接口协议、软件和人员的重要变更需求都已归档。</p> <p>(8) 文档已更新，包括任何来自早期运行经验的更新。</p> <p>(9) 未来开发/试验计划已经完成</p>	<p>(1) 观察到的空间飞行器和科学载荷的性能与预测的一致；若非如此，原因已充分了解，从而有信心预测未来行为。</p> <p>(2) 所有异常已经适当归档，其对运行的影响已经评估。而且，影响空间飞行器健康和安全或影响关键飞行运行的异常已经适当的处理。</p> <p>(3) 使命任务运行能力，包括人员和计划，已经足够适应真实的飞行性能。</p> <p>(4) 作为运行使用准备状态评审一部分，任何关于运行使用的留置已得到满意的处理</p>

16) 关键事件准备状态评审

关键事件准备状态评审确认在飞行运行中，项目执行使命任务关键活动的准备情况。

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-17。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

表 6.7-17 关键事件准备状态评审启动和成功准则

关键事件准备状态评审	
启动 准 则	成 功 准 则
<p>(1) 使命任务总览和关键事件的背景。</p> <p>(2) 活动需求和约束。</p> <p>(3) 关键活动序列设计描述，包括关键权衡和选定方法的基本原理。</p> <p>(4) 故障预防策略。</p> <p>(5) 关键活动运行计划，包括计划的上传链路和关键程度。</p> <p>(6) 序列验证（试验、全程排查、同行评审）和关键活动确认。</p> <p>(7) 运行使用团队培训计划和准备情况报告。</p> <p>(8) 风险区域和缓解方法。</p> <p>(9) 空间飞行器准备情况报告。</p> <p>(10) 未决事项和计划</p>	<p>(1) 关键活动设计遵从需求。</p> <p>(2) 关键活动的准备周到彻底，包括验证和确认。</p> <p>(3) 项目（包括所有系统、保障服务和文档）已经准备好支持活动。</p> <p>(4) 关键事件成功执行的需求是完整的和可理解的，而且已经分解到合适的实施层次</p>

17) 飞行后评估评审

飞行后评估评审在飞行结束后评价飞行中的活动。评审确定所有在飞行和使命任务期间发生的异常，确定缓解或解决未来飞行中的异常所需要的行动。

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品满足启动准则和成功准则。评审的启动准则和成功准则见表 6.7-18。
- 确保评审中发现的问题适当归档并准备好解决方案计划。

表 6.7-18 飞行后评估评审启动和成功准则

飞行后评估评审	
启动 准 则	成 功 准 则
(1) 已确定所有发生在使命任务期间或发生在飞行前试验、倒计时和上升过程中的异常。 (2) 关于回收后全面条件的报告。 (3) 提供任何空间碎片增加的证据报告。 (4) 所有图片和视频文档可用。 (5) 硬件分离后的保留计划已完成。 (6) 飞行后评估的团队运行计划完成。 (7) 拆解活动已经计划和安排完毕。 (8) 协调飞行中异常故障修理和飞行后数据保存的流程和控制方案已经开发。 (9) 问题报告、纠错行动请求、飞行后异常记录和最终飞行后归档已完成。 (10) 所有飞行后硬件和飞行数据的评价报告已完成	(1) 正式最终报告中记录飞行性能和对未来使命任务的建议。 (2) 所有异常已经适当的归档和处理。 (3) 异常对未来飞行运行的影响已经评估。 (4) 保留评估文档和影像的计划已经制定。 (5) 报告和其他文档已经添加到进行性能比较和趋势预测的数据库

18) 退役评审

退役评审确认系统终止或退役的决策，评估系统安全退役和系统资产处置的准备情况。退役评审通常在常规使命任务运行接近完成计划的使命任务目标结束时进行。退役评审也可能提前，如某些计划外事件出现，需要提前终止使命任务；或者推迟，如运行寿命延长，允许进行更多的研究。

目标

评审的目标如下：

- 确保评审是对产品的全面评审。
- 确保产品符合启动准则和成功准则。评审的启动准则和成功准则见表 6.7-19。
- 确保评审中发现的问题适当归档和准备好解决方案计划。

评审结果

成功完成的退役评审确保系统的退役，以及处置事项和过程是适当和有效的。

表 6.7-19 退役评审启动和成功准则

退 役 评 审	
启 动 准 则	成 功 准 则
<p>(1) 与退役和处置相关的需求已经定义。</p> <p>(2) 退役、处置和其他服务活动的终止计划已经准备就绪。</p> <p>(3) 用来支持退役和处置活动的资源已经就位，项目资产的安置计划、使命任务和项目基础数据已经归档。</p> <p>(4) 安全性、环境和其他任何约束已明确。</p> <p>(5) 当前系统能力已明确。</p> <p>(6) 对于异常操作，所有相对于最初期望控制基线的起作用的事件、条件和变更都已描述</p>	<p>(1) 退役处置的原因已经归档。</p> <p>(2) 退役和处置计划是完整的，得到相应管理层的批准，满足 NASA 的安全性、环境和健康准则。针对所有潜在想定包括意外情况的运行计划是完整的并且获得批准。所有需要的保障系统是可用的。</p> <p>(3) 所有人员都已适当进行常规和突发事件技术规程培训。</p> <p>(4) 安全、健康和环境危险都已确定。危险控制方案已经验证。</p> <p>(5) 与处置相关的风险已经确定并适当缓解。残留风险被相应管理层所接受。</p> <p>(6) 如果硬件需从轨道回收：</p> <ul style="list-style-type: none"> • 返回点的活动计划已经定义和批准。 • 需要的设施可用且满足需求，如果需要包括污染控制设施。 • 运送计划已定义且得到批准。运输容器和处理设备，还有污染和环境控制及监测装置是可用的。 <p>(7) 使命任务拥有的资产（如硬件、软件、设施）安置计划已经明确并得到批准。</p> <p>(8) 使命任务数据的归档和后续分析计划已经明确和批准。执行这些计划的安排已经确定。在项目寿命周期中经验教训的获取和分发计划已经明确和批准。已经确定充足的资源（进度、预算和人员），可用于成功完成所有退役、处置和安置活动</p>

5. 其他技术评审

这些典型的技术评审曾在早期的工程和项目中进行，但并不作为 NPR7123.1 系统工程流程所必需的一部分。

1) 设计认证评审

目的

设计认证评审确保合格验证能证明设计遵从功能和性能需求。

时间安排

设计认证评审紧随系统关键设计评审，在合格试验和所有合格评审导致纠正行动所需的修改已完成之后进行。

目标

评审的目标如下：

- 确认验证结果满足功能和性能需求，试验计划和技术规程在指定的环境下正确执行。
- 证明在试验件和生产件之间可追踪性是正确的，包括名称、序号和当前列出的所有免责声明。
- 确定任何在试验开始由于设计或需求变更需要或执行的附加试验，根据试验结果解决相关问题。

成功完成的准则

下列事项组成一个检查清单，帮助确定设计认证评审产品的准备情况：

- 试验件的来源是否直接追溯到生产单位？
- 试验件使用的验证计划是否是新的且得到批准的？
- 使用的试验技术规程和环境是否符合计划所指定的？

- 试验中是否产生试验件技术状态或设计结果的变更？是否需要设计或规范变更，或重新试验？
- 设计和规范文档是否已经审核？
- 验证结果是否满足功能和性能需求？
- 验证、设计和说明文档是否相互关联？

评审结果

作为设计认证评审成功的结果，目标产品设计获得批准生产。所有未决问题应该由终止行动和计划来解决。

2) 功能和物理技术状态审核

技术状态审核认定产品技术状态是精确和完整的。技术状态审核的两种类型分别是功能技术状态审核和物理技术状态审核（见表 6.7-20）。功能技术状态审核检查成型产品的功能特性并根据试验结果验证产品满足其初步设计评审和关键设计评审批准的功能控制基线文档中定义的需求。功能技术状态审核将在硬件或软件成型产品上执行，并先于成型产品的物理技术状态审核进行。物理技术状态审核（可看做是技术状态检查）检查成型产品的物理技术状态并验证产品符合前期由关键设计评审批准的待建（待编）产品的控制基线文档。物理技术状态审核将在硬件和软件成型产品上进行。

表 6.7-20 功能和物理技术状态审核

有代表性的审查数据列表	
功能技术状态审核	物理技术状态审核
<ul style="list-style-type: none">• 设计规范；• 设计图纸和部件清单；• 工程技术变更提议/工程技术变更请求；• 合并和审理中的变更/免责审批请求；• 说明书和图纸目录结构；• 空间碎片控制计划；• 结构动力学、分析、载荷和模型文档；• 材料使用协议/材料鉴别使用清单；• 验证和确认需求、计划、技术规程和报告；• 软件需求和开发文档；• 已完成试验和试验结果列表；• 关键设计评审完成文档，包括评审内容偏差/行动请求和安置报告；• 分析报告；• ALERT（紧急发射事件抑制建议）追踪日志；• 危险分析/风险评估	<ul style="list-style-type: none">• 所有规范的最终版本；• 产品图纸和部件清单；• 技术状态登记和状态报告；• 所有软件和硬件文档的最终版本；• 所有产品功能技术状态审核结论的副本；• 批准的和突出的工程技术变更提议、工程技术变更请求和变更/免责审批请求的清单；• 合同部件清单；• 运行中试验技术规程；• 图纸和规范目录；• 制作和检查“产品建造”记录；• 检查记录；• 产品建造中的异常报告；• 产品日志工作本；• 建成产品的技术状态列表

3) 技术同行评审

同行评审提供确保产品和流程质量的实质技术见解。同行评审是深入聚焦的技术评审，支持产品包括关键文档或数据包的设计和开发。它们通常但不总是作为初步设计评审和关键设计评审等技术评审的辅助评审进行。同行评审的目的是通过引入专家知识和确认方法，辨识缺陷并提出产品改进的特殊建议来增加价值和减少风险。

工程技术同行评审的结果构成评审流程的关键要素。评审中得出的结果和问题在适当的

较高单元层次记录和报告。评审同行应当从项目团队外部选择，但是他们应该具有相似的技术背景，且选择需依据他们的技能和经验进行。

评审同行应该仅仅关注产品的技术完整性和质量。评审同行应该保持简单和非正式，评审应该专注于文档审查，尽量减少图表演示。相对于台前表述方式，圆桌会议形式更受欢迎。同行评审应该给出需要审查事项的所有技术视图。

技术深度应该建立在允许评审小组洞悉技术风险的水平上。需要建立规则来确保同行评审流程的一致性。在做出评审结论时，关于问题、建议和行动的报告必须分发给技术团队。

对于系统工程在外部完成的那些项目，同行评审必须是合同的一部分。

关于建立和进行同行评审的附加指南参见附录 N。

6.7.2.2 状态报告和评估

本小节提供关于状态报告和评估技术的补充信息，评估指标包括成本和进度（包括挣值管理）、技术性能和系统工程流程。

1. 成本和进度控制指标

关于成本和进度的状态报告和评估便于项目负责人和系统工程师查看项目如何根据其计划成本和进度目标进展。从管理的角度看，完成这些目标等同于满足系统的技术性能需求。将成本和进度状态报告和评估看做对“生产系统的系统”的性能度量是非常有用的。

NPR7120.5 提出应用挣值管理支持成本和进度管理的特定需求。挣值管理可用于内部的和合同性的工作。挣值管理系统实施的水平依赖于货币价值及项目或合同的风险。挣值管理系统标准是 ANSI-EIA-748。项目负责人/系统工程师使用其中的指南建立工程和项目挣值管理实施计划。

2. 评估方法

实际测量数据用于评估项目成本、进度安排和技术性能及其对完成项目成本和进度的影响。在工程控制术语中，实际的数据与计划成本或进度状态之间的差异称为“偏差”。偏差必须控制在子系统工作分解结构层对应的控制账目层级。负责这项活动的人员通常称为控制账目负责人。控制账目负责人开发工作和产品计划、进度表和分时段资源计划。技术子系统负责人/领导人通常将这项任务视为其子系统管理责任的一部分。

图 6.7-3 描述了两类偏差、成本、进度表和一些相关概念。面向产品的工作分解结构将项目分解为离散的任务和产品。与每一任务（处于工作分解结构任何层次）和产品相关的是进度和预算（如计划）。对工作分解结构单元，工作计划预算（ $BCWS_t$ ）是计划在 t 时刻完成的任务和产品所有工作的预算总和。工作执行预算（ $BCWP_t$ ），又称挣值（ EV_t ），是在 t 时刻计划中工作分解结构单元实际生产的任务和产品的预算总和。 $BCWS_t$ 和 $BCWP_t$ 之间的差称为 t 时刻进度偏差。负值表明工作落后于进度表。

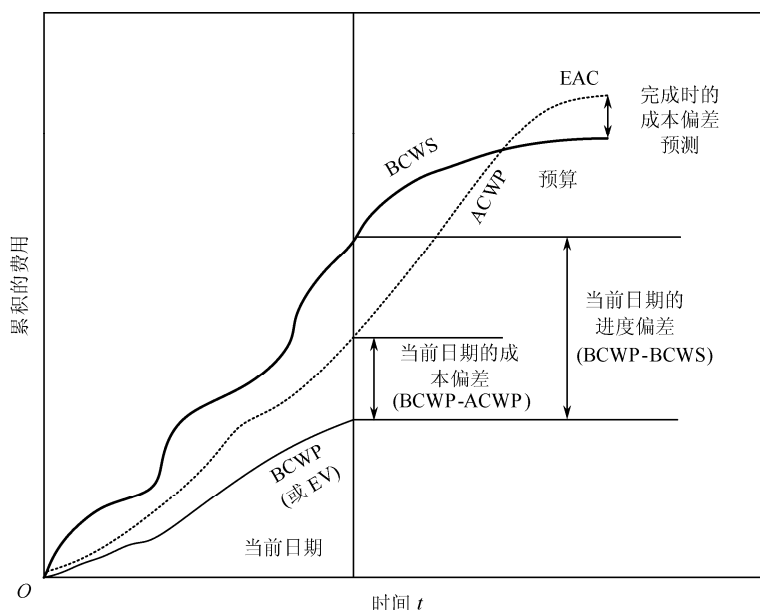


图 6.7-3 成本和进度偏差

工作实际执行成本 ($ACWP_t$) 表示到 t 时刻已为这些工作分解结构单元支出的资金。预算和实际成本的差, $BCWP_t$ 与 $ACWP_t$ 之间的差称为 t 时刻成本偏差。负值表示成本超支。

当进度偏差或成本偏差超出预设的该层控制账目阈值, 表明与控制基线计划显著偏离, 必须对条件进行分析来确定偏差存在原因。一旦对原因有所了解, 控制账目负责人可以预告完成控制账目需要的时间和资源。当纠正行动可行时 (保持在 $BCWS$ 之内), 必须对执行该行动的计划进行分析。若纠正行动不可行, 成本超支或进度延迟可能不可避免。应该牢记的是, 项目团队越早确定进度偏差或成本偏差的技术问题, 越有可能减小对项目完成的影响。

偏差表明项目的完工成本估算 (EAC_t) 可能与完工成本预算 (BAC) 不同。 BAC 和 EAC 之间的差是完工偏差 (VAC)。 VAC 为负值通常是不利的, 而 VAC 为正值通常是有利的。这些偏差也可能指向项目计划完工日期的变更。偏差类型使工程分析人员能在项目寿命周期中任何点上评估 EAC (见关于分析完工成本估算的注记)。这些分析结果应仅用于根据偏差分析过程中的估算进行“明智检查”。

如果成本和进度控制基线及工作的技术范围没有适当定义和完全综合, 则估算当前项目成本 EAC 非常困难 (或不可能)。

其他有效因子可以用性能指标数据计算。进度性能指标 (SPI) 是用货币对工作完成情况的度量。 SPI 用完成工作货币值或 $BCWP$ 除以工作计划货币值或 $BCWS$ 计算。与其他比值一样, 小于 1 表示落后于计划的状况, 等于 1 表示按计划进行状况, 大于 1 表明工作比计划提前。成本性能指标 (CPI) 是对费效的度量, 用一段工作的挣值或 $BCWP$ 与同段工作的完全成本或 $ACWP$ 的比值计算。 CPI 表明为项目花费的单位货币能够完成多少工作。 CPI 小于 1 揭示负的成本效益, 等于 1 为符合成本, 大于 1 为正的效益。注意, 传统度量是计划成本与实际成本对比, 但是, 这样对比从不使用挣值数据。计划和实际成本比较仅表明花费而非整体项目性能。

完工时成本估算分析

EAC 可在项目任何时刻进行估算,应当至少每个月评审一次。EAC 需要控制账目负责人的详细评审。统计估算可用于与控制账目负责人估算的交叉检查并给出估算的区间范围。用来计算统计 EAC 的近似公式依赖于任何可能存在偏差的相关原因。如果偏差因为单次事件存在,如偶然事件,则 $EAC = ACWP + (BAC - BCWP)$ 。CPI 和 SPI 同样应该在开发 EAC 时考虑。

如果留置、行动项或重要问题数量增加,而提高未来工作的难度,EAC 可能比上式估算值有较大比率增长。这些因素可采用 6.4 节描述的风险管理方法解决。

3. 技术指标——效能指标、性能指标和技术性能指标

1) 效能指标 (MOE)

效能指标是对“运行使用”成功的度量,与在确定环境中达到使命任务或运行使用目标密切相关。效能指标旨在关注使命任务或运行使用目标达到程度,而不是如何达到,即效能指标应该独立于任何特定解决方案。同样,效能指标是在权衡研究和决策分析中对每个提议的解决方案“完好度”的评估标准。度量或计算效能指标不仅使备选解决方案能进行定量比较,而且可观察其对与运行环境相关的关键假设及任何性能指标的敏感性(见下文性能指标讨论)。

在系统工程流程中,效能指标应用于如下事项:

- 从客户/利益相关者观点定义高层运行使用需求。
- 在权衡研究中对备选解决方案进行比较和排序。
- 观察计划使命任务或运行成功对关键运行假设和性能参数的相对敏感度。
- 确定使命任务或运行成功的定量目标保持可达,从而推进系统开发流程(见下文技术性能指标讨论)

2) 性能指标 (MOP)

性能指标是与系统相关的物理或功能属性特征的度量,如发动机比冲、最大推力、质量和有效载荷。这些属性通常在特定的试验条件或运行环境下度量。性能指标是达成使命任务或运行成功中重要但不直接度量的属性。通常多个性能指标形成效能指标。性能指标经常称为系统性能需求,当设计方案满足时,导致达到系统效能指标的阈值。

效能指标和性能指标之间的区别在于从不同的观点阐述。效能指标涉及解决方案的效能,从用户/客户/利益相关者表述的使命任务或者运行成功准则出发。效能指标代表利益相关者期望,是判断系统成功的关键,但不能设定为使利益相关者判定系统失败的关键。性能指标是供应商特别设计方案实际性能的度量,该方案可能仅与客户/利益相关者关心的内容间接相关。

3) 技术性能指标 (TPM)

技术性能指标是使命任务的关键成功参数或性能参数,通过比较当前实际达到的参数值与此刻预期值和未来计划值,实现对产品实施执行过程的监控。技术性能指标用于确认进展和识别不足,这些不足可能危及系统需求能否满足或带来项目成本及进度风险。当技术性能指标值落入预期值的期望区间外时,则表明需要进行评价和纠正行动。

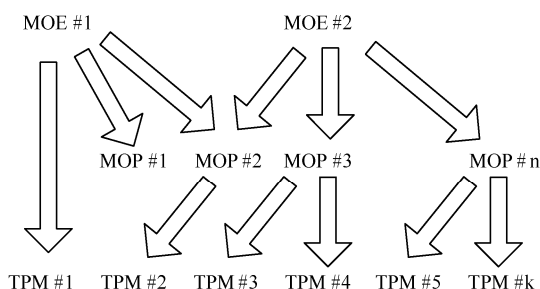
在系统工程流程中,技术性能指标应用于如下事项:

- 预报实施执行过程中主要里程碑或关键事件点关键参数达到的值。
- 确定参数的实际值和计划值的差异。
- 提供相关参数的计划值以便于获得系统效能评估结论。

- 对需要引起管理层注意的潜在风险提供早期预警（当存在负值余量时）。
- 尽早明确能够为减少风险和成本或增加系统效能进行权衡的潜在机会（当存在正值余量时）。
- 支持对提议的设计变更进行评估。

4) 选择技术性能指标

技术性能指标通常从定义的效能指标和性能指标集中选择。应意识到追踪技术性能指标需要资源分配，以及仔细选择一组准确反映关键参数或风险因素并可能被不同设计决策影响的、简明的、可度量的技术性能指标。一般来说，技术性能指标可以是通用的（属性对每个产品分解结构单元有意义，如质量或可靠性）或是单独的（属性仅对特定的产品分解结构单元有意义）。效能指标、性能指标和技术性能指标之间的关系如图 6.7-4 所示。系统工程师需要决定哪些通用和单独的技术性能指标值需要在产品分解结构每层上追踪（见技术性能指标例注记）。在产品分解结构较低层次，需追踪的技术性能指标可以通过针对每个系统、子系统的功能和性能需求确定。



MOE 来自于利益相关者期望的状态；认为对使命任务或者系统运行成功是非常关键的

MOP 主要的物理和性能参数；确保满足相应的MOE所必需

TPM 关键的使命任务成功或者性能属性；可测量；建立、控制和监视进度概况

图 6.7-4 效能指标、性能指标和技术性能指标之间的关系

技术性能指标试图在是否适当满足选定的关键技术参数需求方面为设计提供预警，系统工程师应当选择处于系统效能或使命任务可行性良好（定量）定义界限内的技术性能指标。通常这些界限表示确定的约束上限或下限。空间飞行器技术性能指标的典型示例是它的发射质量，该质量不能超过选定的运载火箭的能力。作为高层技术性能指标追踪发射质量意味着确保该情况不会发生。高层技术性能指标如发射质量，必须经常做预算修正并分配到多个系统单元中。为能找出所有误差源，需要低层次的追踪和报告。

总体上，作为重要状态和评估工具，技术性能指标必须满足的情况如下：

- 是系统的重要描述（如质量、射程、能力、响应时间、安全参数），能在关键事件（如评审、审核和试验）中监控。
- 能够（通过试验、检查、演示或分析）进行度量。
- 能够建立合理的计划进展剖面（如来自历史数据或基于试验计划）。

技术性能指标示例

来自效能指标的技术性能指标

- 使命任务性能（如返回的所有科学数据的数据量）；
- 安全性（如人员损失概率，使命任务失败概率）；
- 可达的可用性（如工作时间与工作时间和停工时间两者之和的比值）；

来自性能指标的技术性能指标

- 预期推力/确定推力的比；
- 预期比冲 I_{sp} /确定比冲的比；
- 任务结束时净质量；
- 发射质量（包括净质量、使命任务所需推进剂+推进剂储备、其他消耗品和上面级质量）；
- 任务结束时推进剂余量；
- 任务结束时其他消耗品余量；
- 使命任务周期的电力余量；
- 控制系统稳定性余量；
- 电磁干扰/电磁兼容易损度余量；
- 飞行任务中数据处理存储器需求；
- 飞行任务中数据处理的解算时间；
- 飞行任务中数据总线容量；
- 总体指示误差；
- 发射时的总质量；
- 有效载荷质量（常规高度或轨道）；
- 可靠性；
- 再次使用需要的平均准备时间；
- 人员维修需要的总时间；
- 系统飞行时间；
- 故障监测能力；
- 系统设计的在轨人员通道比例。

5) 技术性能指标评估和报告方法

系统技术性能指标状态报告和评估有助于成本和进度控制。大量的评估和报告方法已经用于 NASA 项目中，包括计划剖面方法和余量管理方法。

图 6.7-5 给出计划剖面方法用于 Chandra 项目技术性能指标——重量的详细案例。图中描述子系统成分、多种约束、项目限定和从项目系统需求评审到发射的管理储量。

图 6.7-6 给出余量管理方法用于 Sojourner^①项目技术性能指标——质量的详细案例。图中描述余量需求（水平直线）和从工程系统需求评审到发射的实际质量余量。

6) 技术性能指标评估程序与系统工程管理计划的关系

系统工程管理计划是用于描述项目技术性能指标评估程序的通用文档。其中包括需跟踪的技术性能指标的主要列表，以及使用的度量和评估方法。如果用来度量某些高层技术性能指标，则分析方法和模型需要被确定。报告的次数和评估的时间安排同样应该指定。此时，系统工程师必须根据技术性能指标追踪程序的成本来平衡项目技术性能指标追踪的精确性、实时性和有效性需要。

技术性能指标评估程序计划，可能是系统工程管理计划的一部分或大型工程/项目独立文档，应该指定每个技术性能指标分配、分时计划剖面或余量需求、告警区域，以适合选择的评估方法。

① Sojourner Truth 是 19 世纪美国著名的废奴主义者和女权主义者。1997 年 7 月 4 日，美国“火星探测漫游者”飞行器在火星着陆，释放出以 Sojourner 命名的火星漫步小车进行科学实验。“火星探测漫游者”飞行器 1996 年 12 月 4 日由“德尔塔-II”火箭发射升空。

正式的技术性能指标评估程序应完全按照系统工程管理计划制定相应计划并确定控制基线。追踪技术性能指标应在阶段 B 尽早开始。但是，支持全部选定技术性能指标的数据可能直到项目寿命周期后期才可用。在项目寿命周期阶段 C 和阶段 D，技术性能指标的度量应根据系统实际数据的可用性不断精确。

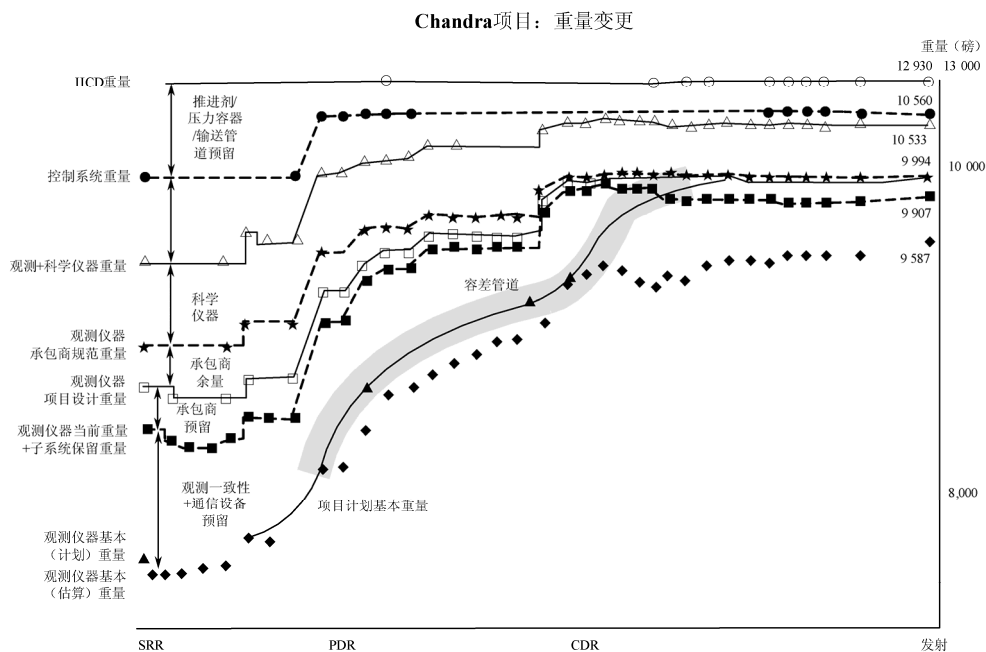
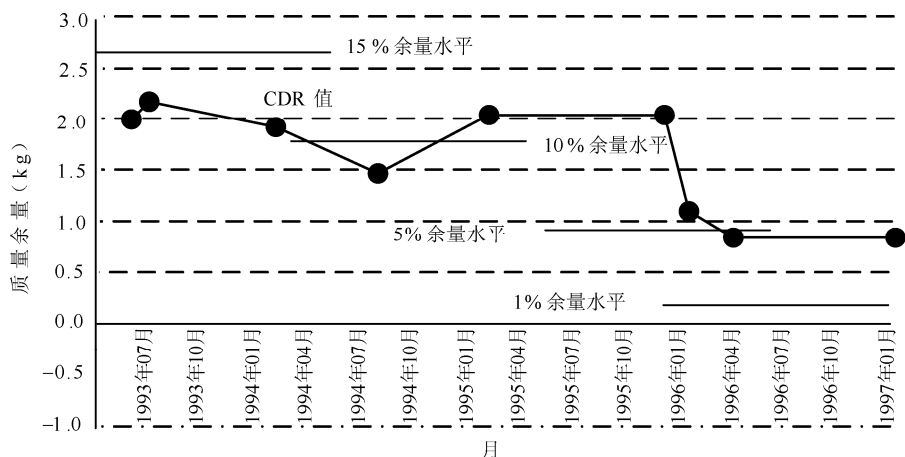


图 6.7-5 计划剖面方法用于重置控制基线的 Chandra 项目技术性能指标——重量



注：当前余量描述：微型着陆系统（着陆车+着陆探测设备）分配=16.0kg；微型着陆系统（着陆车+着陆探测设备）当前最佳估算=15.2kg；微型着陆系统（着陆车+着陆探测设备）余量=0.8kg（5.0%）

图 6.7-6 余量管理方法用于 Sojourner 技术性能指标——质量

对于系统结构的工作分解结构模型，执行的典型活动如下：

- 分析利益相关者期望陈述来构建一组效能指标，由此系统或产品的整体效能可判定，客户满意度同时确定。

- 为每个确定的效能指标定义性能指标。
- 适当定义技术性能指标并在系统工程管理计划中归档技术性能指标评估程序。

4. 系统工程流程指标

系统工程流程指标状况报告和评估为“生产系统的系统”的性能提供更多可视性。由此，这些指标补充了成本和进度控制指标，这些将在本小节讨论。

系统工程流程指标试图量化系统工程流程和组织的效能和生产率。在单独项目中，追踪这些指标使得系统工程师能更好地理解项目的状况和进展。在整个项目中（全时段），系统工程流程指标的追踪促使更好地评估执行系统工程功能的成本和时间。它还使得系统工程组织能证实其不断改进的承诺。

1) 选择系统工程流程指标

一般情况下，系统工程流程指标分成三类：度量系统工作进展、度量流程质量和度量流程生产率。系统工程管理的不同层次通常关注不同的指标。例如，项目负责人或首席系统工程师关注的可能是处理系统工程人员安排、项目风险管理进展和主要权衡研究进展的指标。子系统的系统工程师可能关注于子系统需求和接口定义进展和验证技术规程进展。每个系统工程师仅关注一部分流程指标是有益的。应该追踪哪项指标取决于系统工程师在整个系统工程工作中的角色。值得追踪的系统工程流程指标随着项目寿命周期的推进而变化。

收集和维护关于系统工程流程的数据需要成本。系统工程流程指标状况报告和评估度量活动自身同样需要耗费时间和精力。系统工程人员必须根据流程的成本积累平衡每项系统工程流程指标的价值。这些指标的价值通过对活动提供的无法单独从成本和进度控制指标中得到的深刻理解而有所提升。这些指标也可全时段作为生产力的数据源，其在证实对系统工程工具和培训投入的潜在回报时是宝贵的。

2) 评估方法示例

表 6.7-21 列出部分可用的系统工程流程指标。该列表并非完备的。因为部分指标允许有不同解释，每个 NASA 中心对其做适合自身流程的常识性定义。例如，每个外场中心需要决定“完成”和“批准”需求意味着什么，或这些术语是否相关。作为定义的一部分，重要的是认识到并非所有需求都需集中在一起。对不同类型的需求分别追踪同一个指标可能更有效。

质量相关的指标应当用于系统工程流程中存在超载或故障时提供指示。这些指标可以通过多种方式定义和追踪。例如，需求易变性可量化为新确定的需求数量，或已批准需求的变更数量。又例如，工程变更请求处理可以通过比较未决的累积工程变更请求与处理完毕的累积工程变更请求，或通过描绘未决的时间剖面，或通过比较前一个月未决的工程变更请求与全部未决的数字进行跟踪。系统工程人员应该在选择状态报告和评估方法时使用自身的判断。

生产力相关的指标为单位时间输入相应的系统工程输出提供指示。尽管存在更多成熟的输入指标，最常用的是花费在特定功能或活动上的系统工程小时计量。因为系统工程时间花费不同的成本，应该开发适当的权重方案，确保整个系统工程人工小时的可比性。

进度相关的指标可以用表格和图形显示计划量和实际量，例如，比较验证完毕的计划数量和实际数量。该指标不能与本节中描述的挣值管理混淆。挣值管理关注综合成本和进度的期望水平，而该指标关注的是在子系统、系统或项目中的单个流程或产品。

质量、生产力和进度指标的组合能够提供通常比孤立评价更加重要的趋势。最有用的评

估方法类型是允许比较当前项目的趋势和已成功完成的同类型项目的趋势。后者提供了一个基准，根据这个基准，系统工程师能够判断自己的成果。

表 6.7-21 系统工程流程指标

功 能	指 标	种 类
需求开发和管理	需求确定或需求分析完成或需求被批准	S
	需求易变性	Q
	已计划或已完成权衡研究	S
	批准的需求/每系统工程小时	P
	追踪待声明、待决定或待解决问题，已解决与予以保留	S
设计和开发	规范已计划或已完成	S
	工程技术变更提议/工程技术变更请求的处理	Q
	工程技术图纸已计划或已发布	S
验证和确认	验证和确认计划已确定或已批准	S
	验证和确认技术规程已计划或已完成	S
	功能需求已批准已验证	S
	批准的验证和确认计划/每系统工程小时	P
	问题/失败报告的处理	Q
评审	评审内容偏差的处理	Q
	具体行动处理	Q
其中，S=进展或进度相关；Q=质量相关；P=生产力相关		

6.8 决策分析

本节的目的是给出决策分析流程的描述，包括可选择的工具和方法。决策分析为个人或组织提供进行决策的方法，并提供建立决策问题数学模型和找到最优决策数值解的技术。决策模型能够接受和量化人的主观输入，如专家判断和决策者的偏好。模型的执行可采用简单的手工计算方法，也可以采用诸如复杂的计算机辅助决策程序或决策支持系统。可采用的方法是广泛的，但必须适合所考虑的问题。问题的构成包括必须做出决策选择其一的备选方案，之后可能会发生其中之一的多个事件，以及由决策和事件共同导致的结果。在工程/项目的全寿命周期的各个阶段，决策常常通过不断补充授权的多层结构的小组、委员会和团队做出，其中每个越来越详细的决策受较低层次作出的假设影响。并非所有的决策都需要正式的流程，但是对于确实需要正式流程的决策建立相应流程是重要的。重要的决策及辅助信息（如所作的假设）、工具和模型必须建立完整文档，这样才能结合相应背景评估新的信息和研究已有决策。决策分析流程不断适应这种迭代环境并在项目全寿命周期内进行。

决策分析流程的一个重要方面是考虑和理解何时适宜或需要做出或不做决策。考虑做出决策时，重要的是询问问题，例如，为什么此时需要决策？该决策能推迟多久做出？推迟决策会有怎样的影响？做出决策所需的全部信息可用吗？做出决策之前还有其他必须考虑的关键动因或相关因素和标准吗？

决策者需要在知识不完备条件下从竞争的备选方案中进行决断，决策过程的输出为这一困难工作提供支持；这样，在可行选择中作决断时，理解和记录所有决策工具和方法的假设和局限并将其与其他因素整合是很关键的。

在项目寿命周期早期，做出关于可用技术的高层次决策，如使用固体还是液体火箭推进。

确定运行使用构想、概率和后果，做出设计决策但不指定每个设计方案组件层次的细节。一旦做出高层设计决策，通过嵌套的系统工程流程不断向更低层细化设计直到贯穿整个系统。每个不断细化的决策都受前一次所做假设的影响。例如，固体火箭设计受约束于选择设计方案的决策流程中作出的运行使用假设。这是一个在系统单元之间反复迭代的过程。同样在寿命周期早期，技术团队应该决定在项目的后续阶段支撑决策分析流程所需的数据和信息产品类型。因此技术团队应该设计、开发或采购模型、仿真软件和其他能提供给决策者必要信息的工具。在本节中，讨论在项目寿命周期的不同阶段中，不同层次和不同类型分析的应用。

6.8.1 流程描述

决策分析流程用来帮助评价技术问题、备选方案及其支持决策时的不确定性。图 6.8-1 给出典型的流程流图，包括输入、活动和输出。

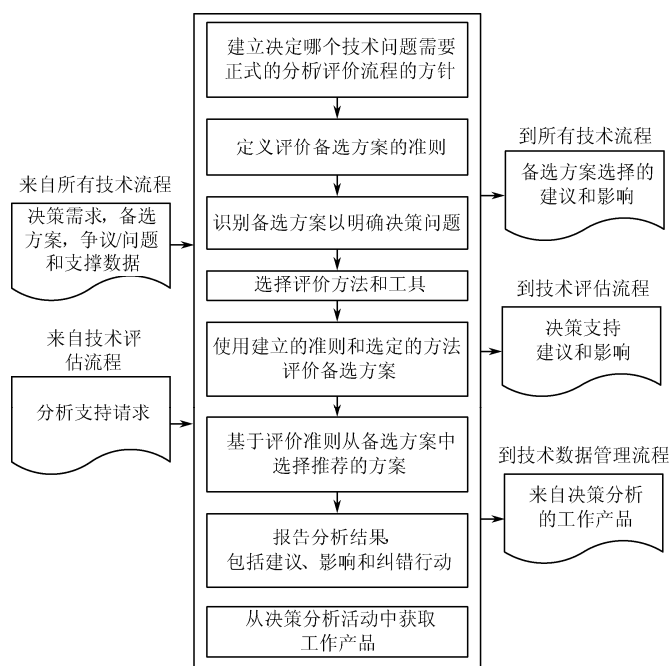


图 6.8-1 决策分析流程

使用决策分析的典型流程如下所述。

- 确定如何分配有限的资源（如预算、人力和动力）到相互竞争的子系统中以达到项目的全局输出最优。
- 通过样本数据，选择和测试评估方法和工具。
- 针对主要变更请求或问题报告的技术状态管理流程。
- 主要设计决策和选择设计方法的设计流程。
- 关键决策点评审或技术评审决策（如初步设计评审，关键设计评审），如 NPR 7120.5 和 NPR 7123.1 中所定义。
- 采用如下描述的“通过”或“不通过”决策（如飞行准备状态评审）：
 - 通过——授权继续推进。
 - 不通过——重做某些特定开发或做更深入研究。

- 主要问题、进度延迟或预算增加的项目管理。
- 主要产品的采购。
- 技术决策。
- 主要风险（如红色或黄色级别）的风险管理。
- 安全性与使命任务担保决策。
- 混合决策（例如，是否该介入项目中处理突发的性能问题）。

在紧急情形下也可采用决策分析。此时，流程步骤、技术规程和会议可以结合起来，决策分析文档可能在流程结束时完成（如在做出决策之后）。然而，在决策期间应该完成并利用决策矩阵。决策分析文档必须在紧急情形发生后尽早完成。

注：研究经常是针对新领域，因此，在进行研究之前，尤其是在大型复杂的决策权衡空间中，试验是否有充足的数据、需要的品质、能否获取决策权等是很重要的。

6.8.1.1 输入

正式的决策分析可能会耗费可观的资源和时间。典型地，仅当下列条件中的某些条件满足时，才能保证其在具体决策中的应用。

- **高收益：**高收益包含在决策中，如有重要意义的费用，安全性或使命任务成功准则。
- **复杂性：**没有详细的分析，备选方案的实际后果很难理解。
- **不确定性：**关键输入的不确定性造成可能的备选方案排序和需要管理的风险评分的实质不确定性。
- **多属性：**属性的数量越多，越需要进行正式分析。
- **利益相关者差异性：**如果利益相关者的价值、偏好和观念存在多样性，则需格外注意弄清目标并形成技术性能指标。

决策分析开始时并不需要满足所有这些条件。关键是需要进行的决策分析工作随上述条件而增加。一旦决策分析流程开始，其输入如下：

- 决策要求，确定的备选方案，问题或难题及支撑数据（来自所有技术管理流程）。
- 决策分析支持的请求（来自技术评估流程）。
- 高层目标和约束（来自工程/项目）。

6.8.1.2 流程活动

对于决策分析流程，进行的典型活动包括如下内容。

1. 建立确定适合正式分析/评价流程中的技术问题主题的指导方针

该步骤需要确定的内容如下：

- 何时使用正式决策技术规程？
- 什么内容需要归档？
- 决策者是谁，他们的责任及决策权是什么？
- 如何处理不需要正式评价技术规程的决策？

决策基于事实、定性和定量数据、工程技术判定和促使信息在分层讨论中流动的公开交流，通过讨论进行技术分析和评估，并做出决策。需要进行技术分析和评估的范围应该与所

需做出决策的问题重要性相称。需要进行正式评价的工作同样重要，必须基于待解决问题的本质确定其适用性。根据所做出决策可能造成后果的量级，确定可用的指导方针。

例如，根据对使命任务成功、飞行安全性、费用和进度的影响，基于风险打分的后果表可用来给适用性赋值。实际使用的数量阈值由决策机构授权给出。表 6.8-1 给出数量赋值的示例。

表 6.8-1 后果表

数 值	后果严重性	正式评价适用性
后果=5, 4	高	强制性的
后果=3	中	可选择的
后果=1, 2	低	不需要的

2. 定义评价备选解决方案的准则

该步骤需要确定的内容如下：

- 所考虑准则的类型，如客户的期望和需求、技术局限性、环境影响、安全性、风险、全部投入和寿命周期费用，以及进度影响；
- 准则可接受的范围和尺度；
- 根据其重要性对准则排序。

决策准则是对所考虑的选择和备选方案单独评估的需要。典型的决策准则包括费用、进度、风险、安全性、任务成功和保障性。然而，专门针对决策的技术准则也应考虑在内。准则应是客观和可测的。准则应允许备选方案之间存在区别。某些准则可能对决策没有意义，然而，它们应该作为考虑因素归档。应区分强制性准则（如“必须……”）和其他准则（如“最好……”）。如果强制性准则不满足，那么相应方案被忽略。对于复杂决策，准则可按范畴或目标分组（见 6.8.2.6 节的层次分析法）。

对准则进行排序和赋权可能是完成决策矩阵中最困难的部分。并非所有准则都同等重要，通常对每个准则赋权来完成排序。为了避免“玩弄”决策矩阵（如通过调整权值改变结果），最好在决策矩阵完成之前确定权值。权值应该只在所有决策参与者一致同意时才能改变。

例如，可简单使用百分比进行排序。设定所有准则的权值相加等于 100。基于准则的重要性进行赋值（较高的百分比表示更重要，如某个准则赋值 50%）。权值需要用百分比形式表示。使用这种方法，百分比最高的选项通常是推荐选项。排序同样可以使用复杂的决策工具。例如，两两比较也是一种决策技术，这种技术通过在准则和选项中成对比较来计算权值。其他的方法如下：

- 构造目标层次和技术性能指标；
- 采用层次分析法，用来说明准则并成对比较；
- 使用技术性能指标权重的基于风险信息决策分析流程。

3. 确定解决决策问题的备选解决方案

该步骤考虑备选方案，包括那些可能伴随问题的方案。

几乎每个决策都有可选择的选项。利用头脑风暴并概要记录可选的决策选项名称。对于复杂决策，最好的做法是查找文献来确定选项。将决策选项减少至合理范围（如 7 加/减 2）。

某些选项显然是不好的，如果考虑这些选项则需要记录。强制准则的使用也可以帮助减少选项的数量。某些决策可能仅有一个选项。最好的做法是对于主要决策记录决策矩阵，即使其只有一个选项（有时什么都不做或者不进行决策也是一个选项）。

4. 选择评价方法和工具

评价方法和工具/技术的选择基于分析决策的目的和辅助方法或工具所用信息的可用性。典型的评价方法包括仿真；加权重衡矩阵；工程技术、制造、成本和技术可行的权衡研究；调查；基于领域经验和原型的外推；用户评审和评议；试验。

使用的工具和技术的选择应该基于分析决策的目的和辅助方法或工具所用信息的可用性。其他的评价方法如下：

- 决策矩阵（见图 6.8-2）；
- 决策分析流程支持、评估方法和工具；
- 基于风险信息决策分析流程；
- 备选方案权衡研究和决策。


决策矩阵 (以电池为例)			输入分数 	延长旧电池的寿命	购买新电池	根据选择的实验收集实验数据	取消实验
准则	强制性 (Y=1/N=0)	权重	数值范围				
使命任务成功（获得实验数据）	1	30	3=最支持 1=最不支持	2	3	3	0
每一个选项的成本	0	10	3=最便宜 1=最昂贵	1	2	3	1
风险（所有选项的风险）	0	15	3=最小风险 1=最大风险	2	1	2	3
时间调度	0	10	3=最少的时间 1=最多的时间	3	2	1	3
安全性	1	15	3=最安全 1=最不安全	2	1	2	3
连续的数据收集	0	20	3=最支持 1=最不支持	3	1	2	1
加权求和（%）		100	3	73%	60%	77%	0%
			数值范围 1~3				

图 6.8-2 决策矩阵示例

5. 根据建立的准则和选定的方法评价备选解决方案

不考虑使用的方法和工具，结果必须包括的内容如下：

- 对与评价准则相关假设的评价和对支持假设正确性证据的评价；
- 针对备选解决方案中属性值的不确定性是否对评价造成影响进行评价。

通过使用图 6.8-2 所示的决策矩阵可进行备选方案与评价准则的比较。评估准则通常位于矩阵左侧一列。备选方案通常处于矩阵的标题行（直到右端）。通常应为每个准则赋予权重。如图示例子中，存在强制性准则。如果强制性准则不能满足，选项的得分就是 0。

当决策准则有不同度量基准时（如数字、货币、重量或日期），可使用归一化为数学运

算建立公共基础。“归一化”过程就是制定统一尺度，使得所有不同类型的准则能够比较或相加。这可以非正式（如低、中、高），按固定差（如取数值 1-3-9），或者使用正式工具进行。无论归一化如何进行，最重要的是牢记尺度要有操作定义。操作定义是可重复和可度量的数字。例如，“高”可能是“概率不小于 67%”。“低”可能是“概率不大于 33%”。对于复杂决策，决策工具通常提供自动归一化方法。必须询问和理解工具的权重和尺度的操作定义。

注：完成决策矩阵可以认为是默认的评价方法。完成决策矩阵是迭代过程。每个准则和选项对应的单元格，需要技术团队完成。使用完成整个决策矩阵需要的评价方法。

6. 基于评价准则从备选解决方案中选择推荐的解决方案

该步骤包括信息的归档，包括所用评价方法的假设和局限性，证明所提出建议的正确性，给出采取所建议行动方案的影响。

通常最高分（如百分比、总分）是建议给管理层的选项。如果建议不同的选项，必须要对为何以较低分数的选项为首选做出解释。通常，如果建议较低分数的选项，则可能最高选项的“风险”或“劣势”极大。有时较低或接近分数的选项收益和优势胜过最高分数者。理想地，所有风险/收益和优势/劣势应作为判剧显示在决策矩阵中，但有时不可能。当建议较低分数选项时，可能是因为赋权或打分不精确。

7. 报告分析和评价的结果和结论包括建议、影响和纠正行动等内容

通常由领域专家组成的技术团队会向 NASA 决策者（如 NASA 委员会、专业组或专家组）提出建议。值得推荐的是由该团队生成白皮书来归档所有主要建议作为陈述材料的备份。可以演示汇报，但是与决策矩阵相关的书面报告更受欢迎（特别是对复杂决策）。决策通常在开会时做出，但也可基于白皮书做出。

8. 从决策分析活动中获取工作产品

该步骤包括获取如下内容：

- 生成的决策分析指导方针和使用的策略及技术规程；
- 分析/评价步骤、准则、方法及使用的工具；
- 分析/评价结果、形成建议中做出的假设、不确定性和推荐行动或纠错行动的灵敏度；
- 总结的经验教训和提高未来决策分析的建议。

在决策报告中能够获取到的典型信息如表 6.8-2 所示。

6.8.1.3 输出

决策分析持续贯穿整个寿命周期。决策分析的产品如下：

- 备选方案选择建议和影响（对所有技术管理流程）；
- 决策支持建议和影响（对技术评估过程）；
- 决策分析活动的工作产品（对技术数据管理流程）；
- 技术风险状态指标（对技术风险管理流程）；
- 技术性能指标，备选方案的性能指标，工程或项目指定的目标层次，决策者的偏好（对所有技术管理流程）。

表 6.8-2 决策报告中能够获取的典型信息

#	章 节	章 节 描 述
1	综合概要	提供一份关于报告的简短的综合概要： <ul style="list-style-type: none">• 建议（简短概述——一句话）；• 需要决策的问题（简短概述——一句话）
2	问题描述	描述需要决策的问题。提供背景、历史、决策者（如委员会、专业组、专家组）和决策建议团队等
3	决策矩阵设置依据	提供设置决策矩阵的基本依据： <ul style="list-style-type: none">• 选定的标准；• 选定的选项；• 选定的权重；• 选定的评价方法。 提供设置完成的决策矩阵副本
4	决策矩阵打分依据	提供决策矩阵打分的基本依据。提供使用选定的评价方法来计算矩阵分数的结果
5	最终的决策矩阵	将最终的表格剪贴到文档中。其中也包含决策矩阵的所有重要的快照
6	风险/收益	对于考虑的最终选项，归档每个选项的风险和收益
7	建议和/或最终决策	描述提供给决策者的建议，描述各选项被选择的基本依据。该节也归档最终的决策
8	不同意见	如果可能，归档任何与所提建议不同的观点。归档不同意见是如何说明的（如决策矩阵、风险等）
9	参考文献	提供所有参考文献
A	附录	提供文献调查的结果，包括总结的经验、前期相关的决策和不同的观点。归档所有用于决策的详细数据分析和风险分析。归档所有决策指标

6.8.2 决策分析指南

本小节的目的是为支持 NASA 的决策分析流程提供指南、方法和工具。

6.8.2.1 系统分析、仿真和性能

系统分析可以在系统全寿命周期背景下更好的理解。全寿命周期背景下的系统分析是对利益相关者在寿命周期中每个阶段需求的响应，从 A 前阶段到阶段 B 直到实现目标产品和更远（见图 6.8-3）。

在维护性能和负担能力要求下，产品系统分析必须支持从产品需求到实现指定产品的转换；能够支持兼容物理需求和功能需求；按可靠性、维修性、保障性、服务性和处置性支持运行使用构想。

系统分析对决策的支持从系统起源到消亡一直发挥作用。这覆盖产品设计、验证、生产、运行维护和处置。以此观点看，寿命周期工程是并行工程的基础。

系统分析应该支持并行工程。在寿命周期早期进行适当的系统分析可以支持规划和开发。本节的目标是支持全寿命周期最优规划的无缝系统分析。例如，寿命周期早期的系统工程能够支持系统在部署、运行和处置方面得到最佳性能。

从历史上看，这样做并不存在问题。系统分析仅仅关注项目所处的寿命周期阶段。后续阶段的系统分析按时间顺序处理。这导致寿命周期阶段后段的主要设计修改非常昂贵。如果

贯穿寿命周期的需求可以同时考虑，并为系统决策者提供结果，资源可以更加有效利用。

图 6.8-3 的寿命周期图显示多种常用类型的系统分析如何适应寿命周期中各个阶段。分析的需求开始于以宽阔的范围和在寿命周期早期阶段需要的更多分析类型，而随着作出决策分析的需求量和范围缩小，项目需求在寿命周期推进过程中逐渐清晰。图 6.8-4 给出一个特定的空间飞行器发射降落场示例，显示特定运行分析输入如何提供与寿命周期中运行部分相关的分析结果。注意：在这里仿真贯穿寿命周期进行，随着项目进展定期更新获取的新数据。

在寿命周期的早期阶段，输入应该包括项目进行过程中合同管理和流程及产品改进时需要的收集定量和定性数据的计划。这个计划应表明需要的数据类型，以决定问题的起因、偏差和异常，提出纠正行动建议来防止重现。这个闭环计划涉及到辨识、解决和循环控制系统，是产生接近预测值的实际可靠性的关键。它应该表明信息技术基础结构和数据库提供数据分类、数据挖掘、数据分析和数据预先管理的能力。问题、不一致和异常的管理应该从数据收集开始，应该是技术评估的主要部分，应该为决策分析提供关键的信息。

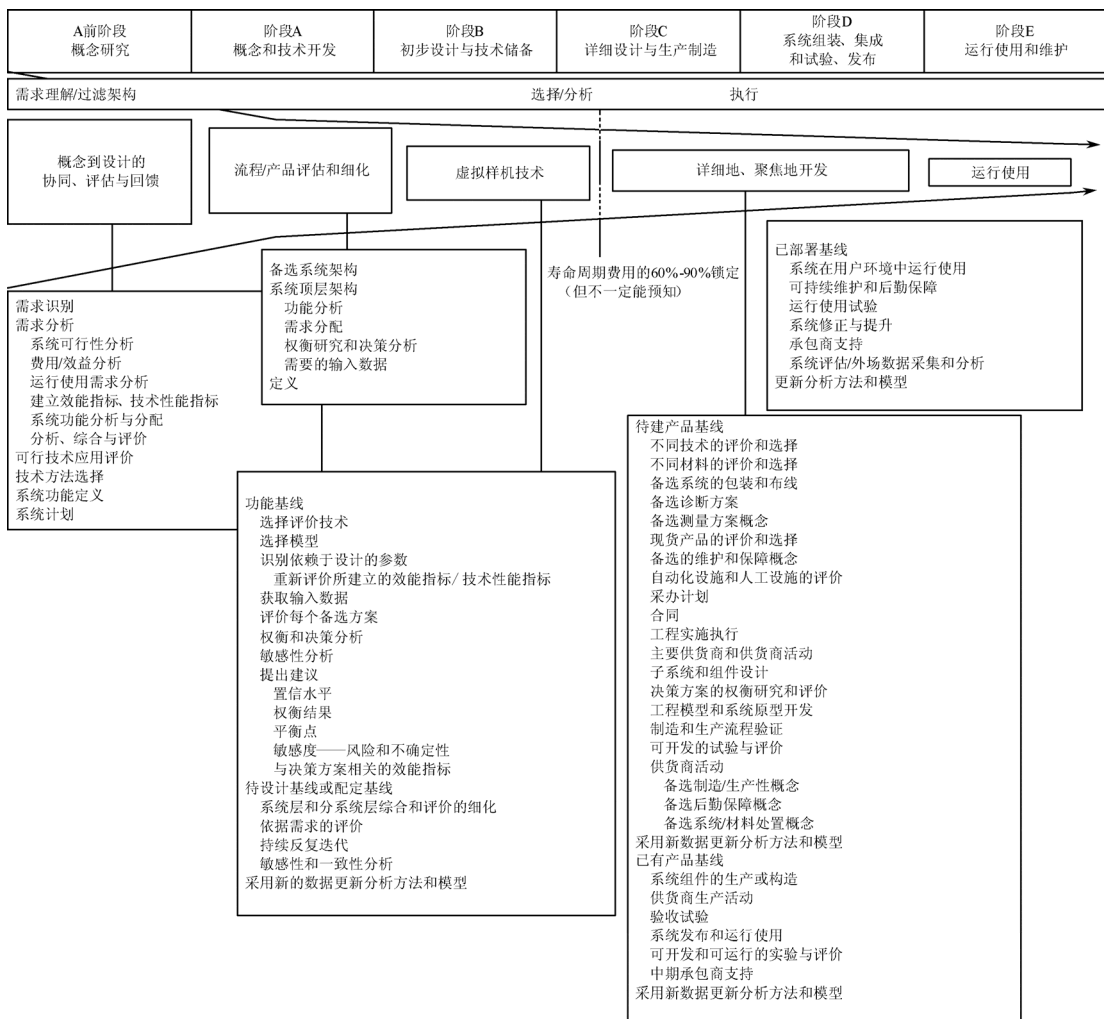
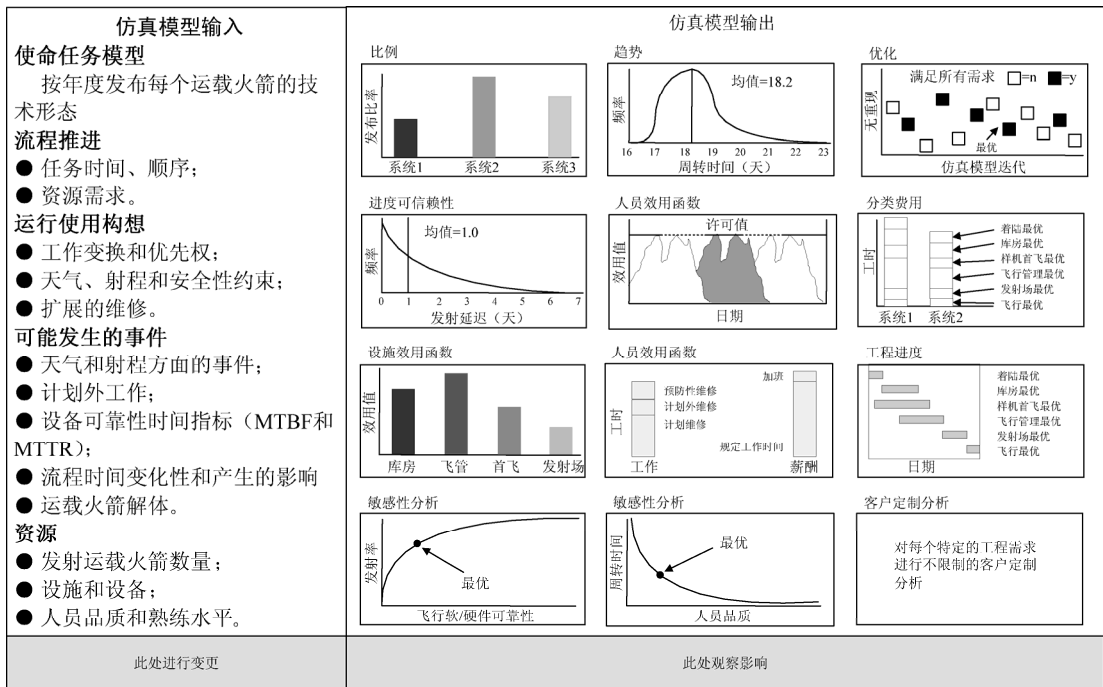


图 6.8-3 贯穿寿命周期的系统分析



该图来自：洛克希德马丁公司 2003 年 11 月为肯尼迪航天中心准备的汇报

图 6.8-4 仿真模型分析技术

6.8.2.2 权衡研究

权衡研究流程是系统工程的重要部分。权衡研究帮助定义在项目各个分辨率层次的衍生出的新系统。本节的关键在于，为了有效权衡研究需要参与人员具备多种技能并共同努力以实现优化系统设计。

图 6.8-5 以最简单形式给出权衡研究流程，首先定义系统的目标和目的，明确其必须满足的约束。在项目寿命周期的早期阶段，目的、目标及约束通常以通用的方式表述。在项目寿命周期后续阶段，当系统架构和设计的某些方面已经确定时，目标和目的可能被陈述为部段或子系统必须达到性能需求。

在系统结构的各个层级，系统工程师需要理解目的、目标与约束的完整含义以形成恰当的系统解决方案。这一步通过功能分析实现。“功能分析”是识别、描述和关联系统必须实现的功能，以完成其目标和目的，在 4.4 节已作详细描述。

与定义目的和目标及进行功能分析紧密联系的步骤是根据实用情况定义系统效能、系统性能及技术属性、系统成本的指标与度量方法（与 2.3 节的讨论统一，这些变量统称为输出变量。某些系统工程书籍又称这些变量为决策准则，但注意不能与下文中描述的“选择规则”相混淆。2.5 节和 6.1 节更详细讨论系统成本和效能的概念）。指标与度量方法的定义，开始于权衡研究流程的解析部分，应使用熟悉的定量方法中的指标和度量方法。

对于每个指标，重要的是考虑如何计算定量指标，即采用什么样的测量方法。如此做的原因是这一步骤将明确那些对达到系统目的和目标至关重要的变量。在实际构建系统之前以系统效能、基本性能和技术属性、系统成本为指标评价该系统备选方案，通常需要使用系统数学模型及其他类型模型。因此，确定度量方法的另一个目的是明确所需模型。

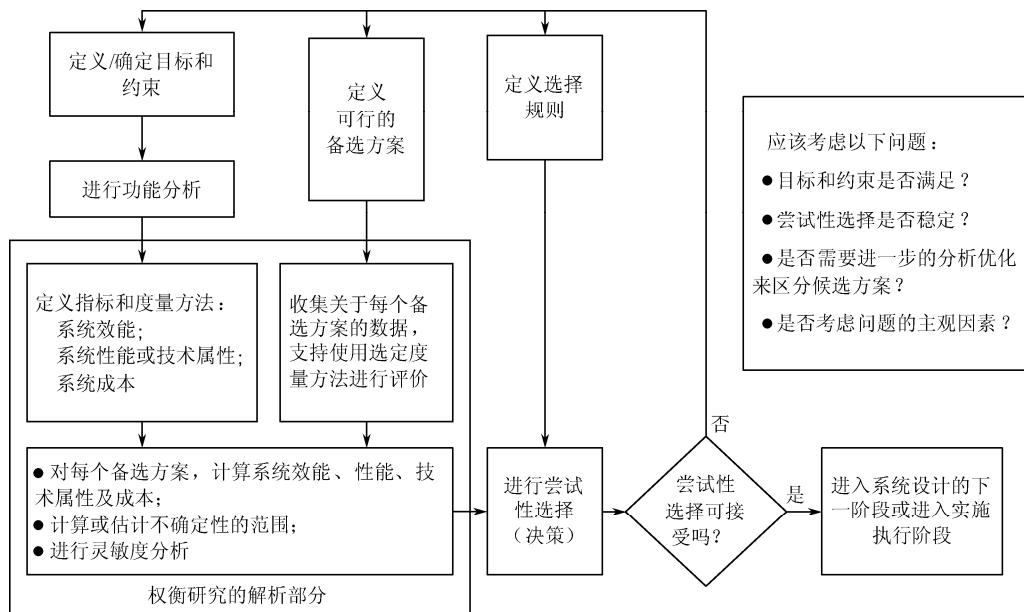


图 6.8-5 权衡研究流程

有时这些模型可以从前期类似性质项目中获得，有时需要新的开发。对于后一种情况，定义度量方法应当触发系统建模活动。由于开发新模型需要相当长时间的工作，需要尽早辨识以确保这些模型能在权衡研究中正式应用。选择规则的定义，是明确如何基于输出变量对备选方案做出（试探性）取舍选择的过程。例如，一个选择规则可以是成本（以某个给定概率）低于 X 美元，满足安全性需求，也可能是在满足某些政治上或进度上约束的备选方案中，选取系统效能估算最高的方案。选择规则的定义，本质上是决定如何做出选择。该步骤独立于系统效能、系统性能、技术属性及系统成本的实际指标。

选择规则有许多。在特定的权衡研究中，选择规则可能取决于进行权衡研究的相关背景——特别是，系统设计建立在系统哪个分辨率层级。在系统设计的各个层级，选择规则通常仅在较高层级选择规则建立之后在其指导下确立。系统设计低层级中权衡研究的选择规则应当与高层级的选择规则一致。

定义可行的备选方案，是创立有可能达到系统目的和目标的备选方案的步骤。该步骤依赖于（在适当详细的层次）对系统功能需求及运行使用构想的了解。通过运行使用时间控制基线或可参照使命任务来促成备选方案，是确定其是否能够真正达到系统需求的有效途径（有时，需要分别建立行为模型以确定各种刺激及控制因素作用或遇到特定环境时系统的响应。这样可完全确定备选方案是否能够真正达到关键的时间及安全需求）。定义可行备选方案，还需要充分了解系统决策时的现有技术，以及可能的新技术。每个可行备选方案都应有定性的文档描述。这些描述文档至少要包含系统功能到备选方案较低层级或设计组件（如子系统）的明确分配。

对备选方案进行权衡研究的一种途径是利用权衡树。

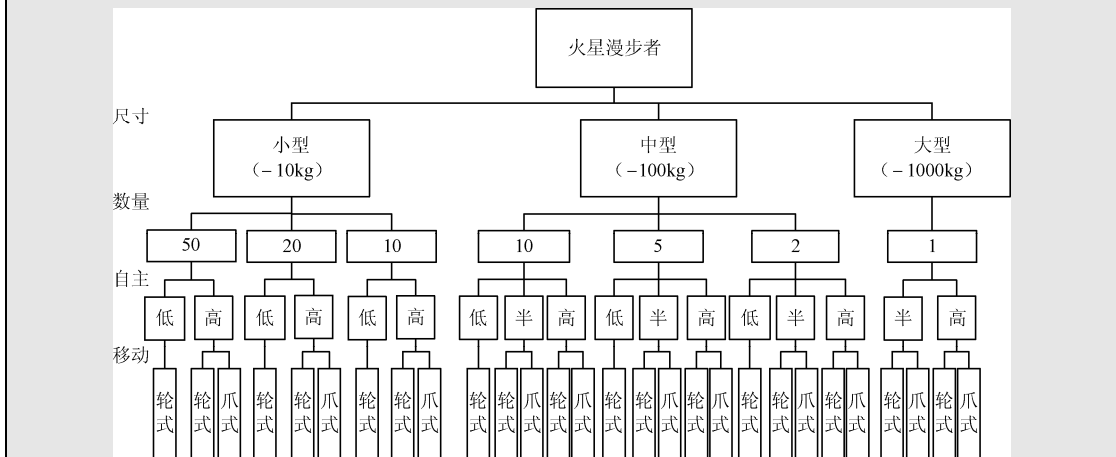
在阶段 A 的权衡研究中，权衡树应包含多个备选系统高层架构以避免过早局限于一种方案。随着系统工程流程的推进，包含不可取备选方案的权衡树枝将被“修剪”掉，更具体的系统设计被添加在那些可取的分支中。修剪不可取备选方案的过程有时称为“杀手式权衡”（参见权衡树注记）。

给定一组可行的备选方案，下一步是数据采集以利用选定的度量方法支持指标评价。如果使用模型计算某些指标，获取模型的输入将为数据采集活动提供动力与导向。通过提供数据，使可靠性、维修性、生产力、综合后勤保障、软件、试验、运行使用和成本等领域的工程师在权衡研究中发挥重要支撑作用。然而，数据采集活动应当由系统工程师策划。该步骤的结果，应当是每个备选方案的定量与定性结合的描述。

每个备选方案的试验结果可特殊使用。在系统工程流程的早期，性能与技术属性通常不确定而需要估计。来自硬试样和软试样试验台的数据可以对模型输入取值范围是否正确提供更多证据。这种信心通过不断收集有关已有系统的数据得到增强。

火星漫步者的权衡树示例

下图显示无人火星漫步系统权衡树的一部分，其目的是寻找合适的载人着陆点。其中每一层表示为确定系统最佳方案需进行权衡研究处理的若干方面。某些备选方案因技术可行性、运载火箭约束等原因被淘汰。备选方案的数量由该树的末端节点数量给出。尽管仅有少数几层，备选方案数量仍快速增加（该树已经修剪淘汰低自动化大尺寸漫步者）。随着系统工程流程推进，不可取的权衡研究结果对应的树枝被放弃。剩余树枝确定需进行更详细权衡研究后才进一步开发。（留下的）备选方案的全族可以用连续变量在权衡树中表示。在本例中，漫步者速度和范围亦可如此表示。通过如此处理变量，可采用数学优化技术。注意权衡树实质上是没机会节点的决策树。



权衡研究流程的下一步是通过计算系统效能、性能、技术属性，以及成本的估计值，量化系统的输出变量。如果需要的数据及其采集、度量方法（如模型）已经确定，理论上该步骤是机械的。实际中，得到有意义的结果常常需要相当的技巧。

理想情况下，所有输入值都精确已知，模型能准确预测输出变量。这实际上不可能，系统工程师需要对每个备选方案的结果变量进行点估计，并计算或估计其不确定性范围。对每个不确定的关键输入，应估计其取值范围。使用输入值范围，可以评估输出变量敏感性并计算其不确定性范围。系统工程师使用蒙特卡洛仿真可得到有意义的概率分布；而当此不可行时，系统工程师就只能接纳取值范围及敏感性。关于不确定性的更多信息参见 6.8.2.8 节中基于风险信息决策分析流程。

如此基本完成权衡研究流程的分析部分。下一步可看做是决断过程。结合选择规则及分析活动的结果，系统工程师能够对备选方案按偏好从高到低进行排序，作为尝试性选择的基础。

尝试性选择不能盲目接受。在多数权衡研究中，需要满足考虑大量问题的结果“真实性检验”。目的、目标及约束是否真的满足？尝试性选择是否严重依赖于度量方法的特定输入值范围，或控制在输入值的合理范围内？（对于后者，尝试性选择称为鲁棒的。）是否有充分数据支持尝试性选择？度量方法是否有充分能力保证尝试性选择结果优于其他备选方案？决策问题的主观方面因素是否充分体现？

如果答案支持尝试性选择，系统工程师能够有更充足的信心建议将系统设计推进到更详细层次，或进入设计实施执行阶段。权衡研究过程产生的对系统效能及相应的性能、技术属性和系统成本的估计，可作为进一步分析的输入。权衡研究流程的分析部分通常给出系统必须达到的性能、技术和费用属性最低标准的量化方法。这些可以被标准化为系统的性能需求。

如果真实性检验没有通过，权衡研究流程将返回到前一步或前几步。基于权衡研究中产生的新信息，这个回退可能导致目的、目标和约束的变更，导致新的备选方案或选择规则的变更。真实性检验可能导致决策变化，应首先改善评价备选方案的指标及度量方法，然后重复权衡研究流程的分析部分。

1. 控制权衡研究流程

权衡研究流程控制有许多机制。其中最重要的是系统工程管理计划。系统工程管理计划确定项目寿命周期各个阶段进行的主要权衡研究。它同时应阐明权衡研究报告的一般内容，从而形成部分决策支持材料（即与正式评审和变更请求同时提交的文档）。

控制权衡流程的第二个机制是选择研究团队领导及成员。由于权衡研究是艺术与科学的结合，研究团队的组成和经验是权衡研究最终有效的决定性因素。选择不同技术背景的研究团队成员是避免过早关注于某个特定技术设计的实用技巧。

权衡研究报告

应该为每次权衡研究准备权衡研究报告。权衡研究报告至少应该明确如下：

- 待分析的系统；
- 系统目的和目标（或需求，到适当的分辨率层次），以及约束；
- 使用的指标和度量方法（模型）；
- 所有使用的数据资源；
- 为进行分析选定的备选方案；
- 计算结果，包括不确定性范围和进行的灵敏度分析；
- 使用的选择规则；
- 推荐的备选方案。

权衡研究报告应该作为系统档案的一部分来维护，从而确保在系统工程流程中所做决策的可追溯性。这些报告使用通用格式，从而更容易审查和将其纳入正式的变更控制流程。

另一个机制是在进行权衡研究中限制备选方案的数量。这一数量通常由进行研究可用的时间和资源决定，因为定义更多备选方案及从中获取所需数据需要的工作量很可观。当然，关注过少或过分类似的备选方案将无法达到权衡研究流程的目的。

控制权衡研究的第四个机制是在研究中使用（或有意不用）模型进行。最后，选择规则的选取同样会对权衡研究流程的结果产生巨大影响。在项目寿命周期中如何应用权衡研究的不同示例参见附录 O。

6.8.2.3 成本收益分析

成本收益分析用于在等价成本或收益下比较备选方案的优劣。该分析取决于正面因素相加及负面因素相减而确定的净值。成本收益分析最大化净收益（收益减去成本）。成本收益分析发现、量化并添加所有的正面因素，这些反映收益；同时发现、量化并减去所有的负面因素，反映成本。两者之差表明计划的行动是否是优先的备选方案。做好成本收益分析的实用技巧是确定所有成本及收益，并适当量化它们。对外部强加的成本上限，采用的方法是基于给定成本上限将效能最大化。费效分析是系统化的定量方法，用于比较为达到特定目标的同等效益下不同方案的成本。基于对各备选方案的寿命周期费用分析，如果项目按现价水平获得给定量的收益时花费最低，则称项目是经济有效的。

无论考虑备选方案提供的收益结算值是否现实，费效分析都是可行的。实际情况是，各个备选方案有时有可用货币表示的相同寿命周期收益，有时有相同的寿命周期效益但无法用货币结算值表示其收益。在基于使命任务和其他需求确定的项目范围内，且完成备选方案成本与收益的辨识、量化和估价后，下一步是找出能达到项目目标且成本最低或最经济有效的备选方案。通常需要备选方案选项和设计的对比分析，如图 4.4-3 所示。一旦确定备选方案具有相同的收益，可以通过估计各方案之间的相对收益率进行比较。最低成本分析着眼于确定满足技术需求的成本最低的项目选择方案。最低成本分析包括比较各种技术可行方案的成本，并选出成本最低者。项目方案必须以不同途径实现使命任务目标。如果存在不同的结果或品质，常规做法是以选择方案相对于另一个方案的收益折算为其中一个不能满足全部使命任务目标的成本，以确保公正比较。折算因子的计算和转换技术规程必须清晰，通过比较项目备选方案的全寿命周期费用和计算成本差异的补偿因子确定最低成本项目方案。所有比较中具有最高补偿因子的项目方案即最低成本备选方案。

费效分析同样处理达到使命任务需求的不同方法。然而，其结果可能仅是间接估计。例如，考虑用于采集科学数据的不同类型系统。每个备选方案的效能针对采集科学数据的不同方法来度量。本例中费效分析度量每个备选方案科学数据增长与其所需成本的比值。最经济有效的方案是以最低成本增加给定量的科学数据。如果选定此方法并应用到所有类似备选方案中，则能以最低成本获得同样的科学数据的增量。然而需注意，最经济有效的方法不必是满足使命任务目标的最有效果方法。其他方法可能最有效果，但同样耗费更多，而不是最经济有效的。费效比，即对所有方法每增加单位计量科学数据的成本，可以比较出最有效果方法的实施需多花费多少。这样，选择哪个方案实施同时取决于所期望的使命任务目标和实施最有效果方案的额外成本。

可能存在项目备选方案有多个结果的情况。评估不同备选方案的效益，需要设计出试验系统，使得不同因子的结果可以累加。同样需要确定不同元素相加时的权重，反映出它们与项目目标的相关重要度。此时，效益分析被称为加权的效益分析。该分析方法在项目备选方案比较中引入主观因素、权重，两者同被用于确定最经济有效的备选方案并确定实施最有效果备选方案的额外成本。

6.8.2.4 影响图

影响图（又称决策网络）是用紧凑的图形与数学表示决策状态（见图 6.8-6）。作为一种

直观的易于理解的决策分析方法，影响图诞生于 20 世纪 70 年代中期。如今，影响图被广泛应用并成为决策树的替代方式，尤其当变量模型的分支数呈指数方式增长时。影响图允许对团队成员共享不完全信息用于构建模型及直接求解，因而可以直接应用于团队决策分析。其基本要素如下所述

- **决策节点：**表示决策输入，以及直接受决策输出影响的事项；
- **机会节点：**表示影响偶然输出的各种因素，以及受偶然输出影响的事项；
- **值节点：**表示影响值的因素，以及受值影响的事项；
- **箭头：**表示各种要素之间的关系。

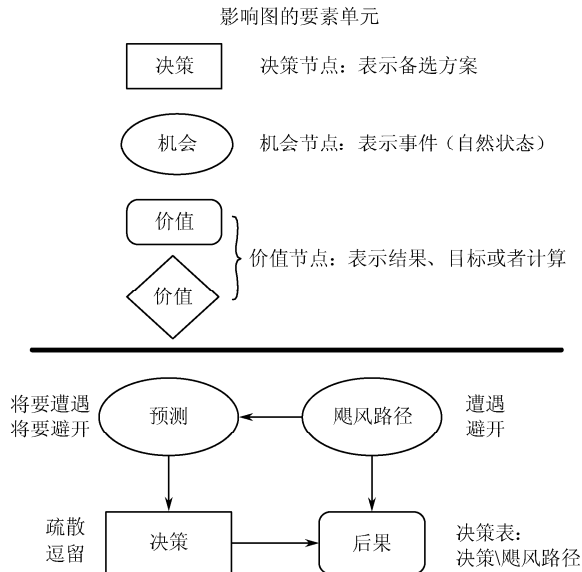


图 6.8-6 影响图

影响图不描述严格的顺序流程。相反，它反映特定点的决策过程，表明所有与决策相关的重要因素。特定模型的影响图并不唯一。影响图的优势在于它能够清晰紧凑地体现决策问题的结构，从而有助于项目沟通和分析人员在确定问题时理清思路。影响图可以通过量化转化为决策树。

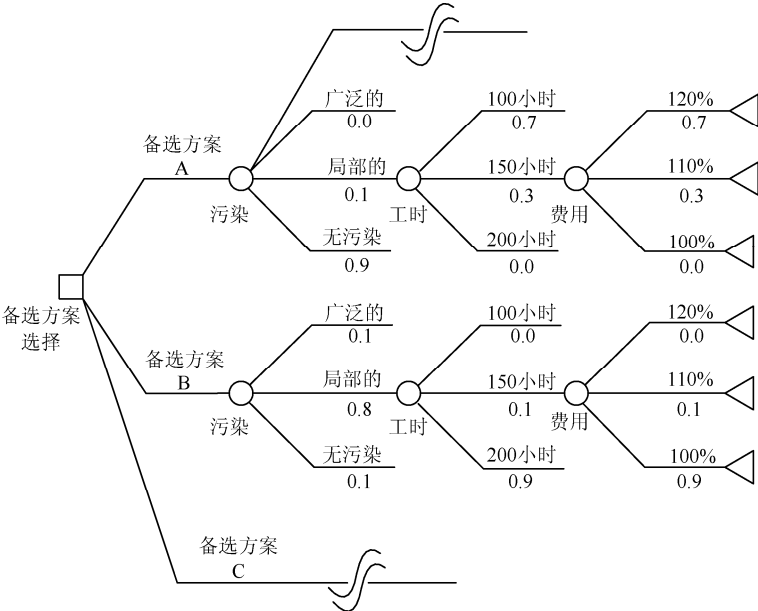
6.8.2.5 决策树

与影响图类似，决策树描绘决策模型，但其着眼点与影响图有所不同。决策树通过离散化所有“机会”节点找出每个决策方案期望的结果，并基于该离散化结果，计算所有方案的各种可能结果并赋予相应的权重。最终通过累加相应底层状态的输出变量（效能指标或期望效用）确定优先的方案。

决策树从左至右水平扩展，其根在最左侧。通常，决策者可用的备选方案起源于最左边的树根。沿着决策树，决策者将遇到基于不同概率结果的分支及可能的新决策节点。因此，决策树的分支从左至右阅读。在决策树的最右端，技术性能指标评分矢量在每个末端列出，标识所有决策输出及机会输出。基于技术性能指标评分，以及选定的选择规则，将确定优先备选方案。

即使是不十分复杂的问题，决策树也将很快变得难以理解。如图 6.8-7 给出决策树示例，

图中只是简化描述，完整的决策树包含更多的分枝并扩展到分析所需的足够详细层次。经常采用的策略是首先画出等价影响图。这常常可以帮助理解首要问题。某些软件包能够帮助轻松构建影响图，并基于所构建的影响图，自动绘出决策树。如果需要，决策树可以被编辑。通常，决策计算基于决策树本身。



6.8.2.6 多目标决策分析

1. 层次分析法（AHP）

层次分析法是由萨蒂（Thomas Saaty）首次提出的。AHP 是一个已经证明有效的处理复杂决策问题的多属性方法，可以帮助决策者选择并明确准则，分析收集的与准则相关的数据，并实施决策流程。通过 AHP 的数学方法可以处理很多不同问题。层次分析法帮助获取主观与客观评价指标，并为检验团队所提备选方案与评价指标的一致性提供有效的机制，从而减少决策中的偏见。

层次分析法基于两两对比分析，可以辅助整个决策流程。通常，层次分析法的 6 个步骤如下：

- 描述所考虑各备选方案的概要。
- 列出一组高层次的目标。
- 从一般到特殊分解高层次目标，用于创建目标层次。
- 通过面谈和问卷等形式由相关专家评分，对各评价目标和属性赋予相应权重，从而确定评价目标的相对重要性。
- 由每位专家针对与技术性能指标相关的决策备选方案进行两两对比，并对每个技术性能指标重复进行。用数学方法，通常用实用软件，合并主观评价结果，对备选方案排序。
- 重复循环面谈/问卷和 AHP 评价流程，直至获得一致的评分排序。

如果层次分析法仅用于构建性能指标和效能指标计算的技术性能指标权重时，只进行上述前 4 个步骤。

使用层次分析法，达到一致性要求可能很快，也可能需要几轮循环。反馈内容包括每个评价者、群体对每项方案的排序，排序差异的原因，以及出现分歧的领域。专家可以选择改变其对技术性能指标权重的判断。此时，需确定不同偏好以便更详细研究。层次分析法假设存在隐含的有大小和方向的偏好矢量，通过两两比较显现出来。这个有力的假设最多只适用于参与专家。备选方案的排序是专家判断的结果，并且不必是一个可重现的结果。关于层次分析法的更多信息，参见萨蒂的著作《层次分析法》。

2. 灵活性与扩展性

对于某些决策，特殊决策方案的选择时有些内容可能在较长的时间内难以建立模型。在这种情况下，可将问题分解成一系列相关的决策，基于当时获取的信息，某些决策在近期做出，而其他决策则需在更晚的时候进行。将决策推迟到将来获得更多信息时进行是有价值的。某些技术选择可能失去这样的机会，而对另一些选择则能够保留这些机会。

在这种情况下，“灵活性”与“扩展性”就显得十分重要。灵活性指能够适应多种应用的能力。扩展性指能够扩展到其他应用中的能力。例如，选择支持探月的系统架构时，可能考虑其拓展到火星探测使命任务。反映了发射到特定轨道质量硬性限制的技术选择明显比适应发射更多种质量的选择灵活性更少。明确将灵活性和扩展性添加到赋权和评价的指标中有利于系统地看待问题。在此应用当中，扩展性和灵活性代表着某些未来的性能指标。

6.8.2.7 效用分析

“效用”是对备选方案所得相对价值的度量。针对该指标，决策团队关注效用的增加或降低，并就增加效用方面解释备选方案决策。理论上，效用的度量单位是 *util*。

效用函数将技术性能指标的范围映射到相关的效用范围上，获取决策者的偏好与风险取向。很容易将评价取值范围简单线性映射到效用轴的 $[0,1]$ 区间内，但这通常不能获取决策者的偏好。决策者的风险取向可能是凸性的（风险趋向型）、凹性的（风险规避型）或两者都有。效用函数直接反映决策者对待风险的态度。在根据效用值对备选方案排序时，在预期性能相同的情况下，相对于性能，其具有较低不确定性的方案，风险规避型决策者倾向于将具有较高不确定性的方案排在较低位置。而风险趋向型决策者则可能给出相反的结果。在对所使用的效用函数进行评估时，检查其结果与决策者偏好的一致性是很重要的（例如， TPM_1 和 TPM_2 的中间值是否被认为意味着最终出现较高的 TPM_1 值和较低的 TPM_2 值）。

图 6.8-8 所示是技术性能指标“体积”的效用函数示例。这项指标被用于空间使命任务的传感器设计。飞行器中体积是珍贵的指标。体积越小越好，相比于相同体积具有高度不确定的方案，决策者倾向于稍稍大数千毫升但高度确定的方案。

在不需要正式处理风险取向时，价值函数可以替代效用函数。价值函数与效用函数相似，但有一点不同。价值函数不考虑决策者的风险取向。它们都不反映决策者对确定结果和不确定结果的对比。

技术性能指标价值函数的评估相对直接。技术性能指标范围的“最佳”端赋值为 1，“最差”端赋值为 0。决策者在技术性能指标可能的取值空间上建立偏好结构，对其中的对应点进行直接评估。效用函数可以看成为价值函数，但价值函数不一定能看成效用函数。

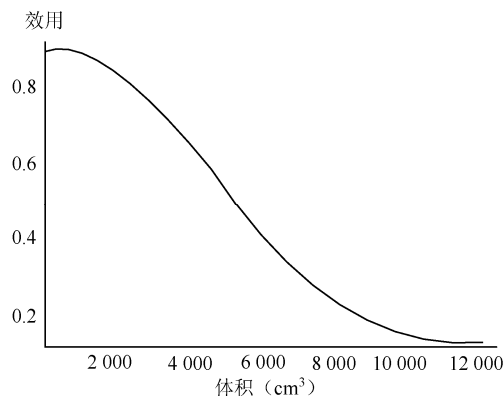


图 6.8-8 性能指标“体积”的效用函数

使用多属性效用理论是对备选方案排序的途径之一。其中，每个备选方案的期望效用被量化，并据此对备选方案排序。

有时，期望效用可以看做性能指标。用此方法的最大好处是当决策者需要考虑风险时，这是处理显著不确定性的最佳方法。概率方法也可用于处理不确定性，这种方法的不足是其需要量化决策者的风险取向。顶层系统架构决策是恰当应用多属性效用理论的典型例子。

6.8.2.8 基于风险信息决策分析方法实例

1. 引言

决策矩阵用于多个决策，但可能不适用于非常复杂的决策和风险决策。对于某些决策，需要特定的工具处理复杂性。本节描述具体的用于支持风险决策分析的决策分析方法。

实践中，决策常采用许多不同方法。简单的方法或许可用，但认清其局限性并在有保证时采用更好的分析方法是重要的。当面临重要量值不确定时，由某些决策者确定该量值的最佳估计，并假设该估计值是正确的，可以称为“争取最佳结果”方法。不幸的是，当代价过高且不确定性过于显著时，最佳方法可能导致不良决策。

基于风险信息的决策分析方法流程如下：

- 论证目标层次结构，技术性能指标。
- 提出和明确备选方案。该流程的备选方案与其他系统工程流程确定的备选方案结合，包括设计方案定义流程、验证、确认和生产等流程。
- 决策方案的风险分析和备选方案排序。
- 认真研究并推荐决策备选方案。
- 密切跟踪决策实施过程。

这些步骤通过首先关注目标，其次再根据目标开发决策备选方案，或采用已经在其他系统工程流程中开发的决策备选方案，支持做出良好决策。决策分析方法的后几个步骤与技术风险管理流程紧密相关，如图 6.8-9 所示。这些步骤包括决策备选方案的风险分析，基于风险分析结果的评议，向决策者推荐建议决策方案。决策的实施过程同样重要。

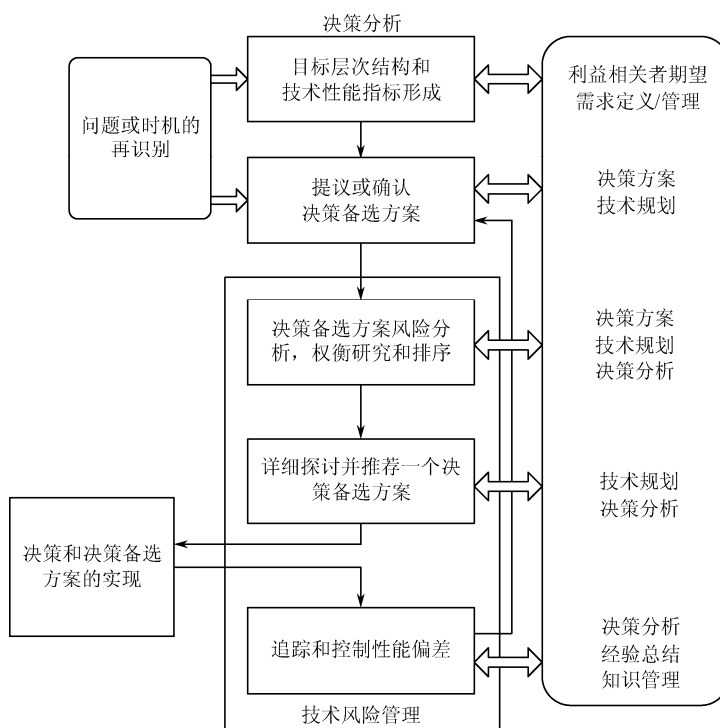


图 6.8-9 基于风险信息的决策分析流程

2. 目标层次结构/技术性能指标

如图 6.8-9 所示，基于风险信息的决策分析始于确立目标层次结构。基于该层次结构，可建立技术性能指标来量化关于工程目标的决策性能。技术性能指标应当具有以下性质：

- 可以支持主要决策备选方案的排序；
- 足够详细以直接用于风险管理流程；
- 优先独立，也就是说技术性能指标对工程目标单独起作用。这一性质有助于保证备选方案排序的恰当性。

图 6.8-10 给出目标层次结构的一个实例。其细节可能随工程的不同而变化，但图 6.8-10 所示的结构不受工程特定目标的影响。

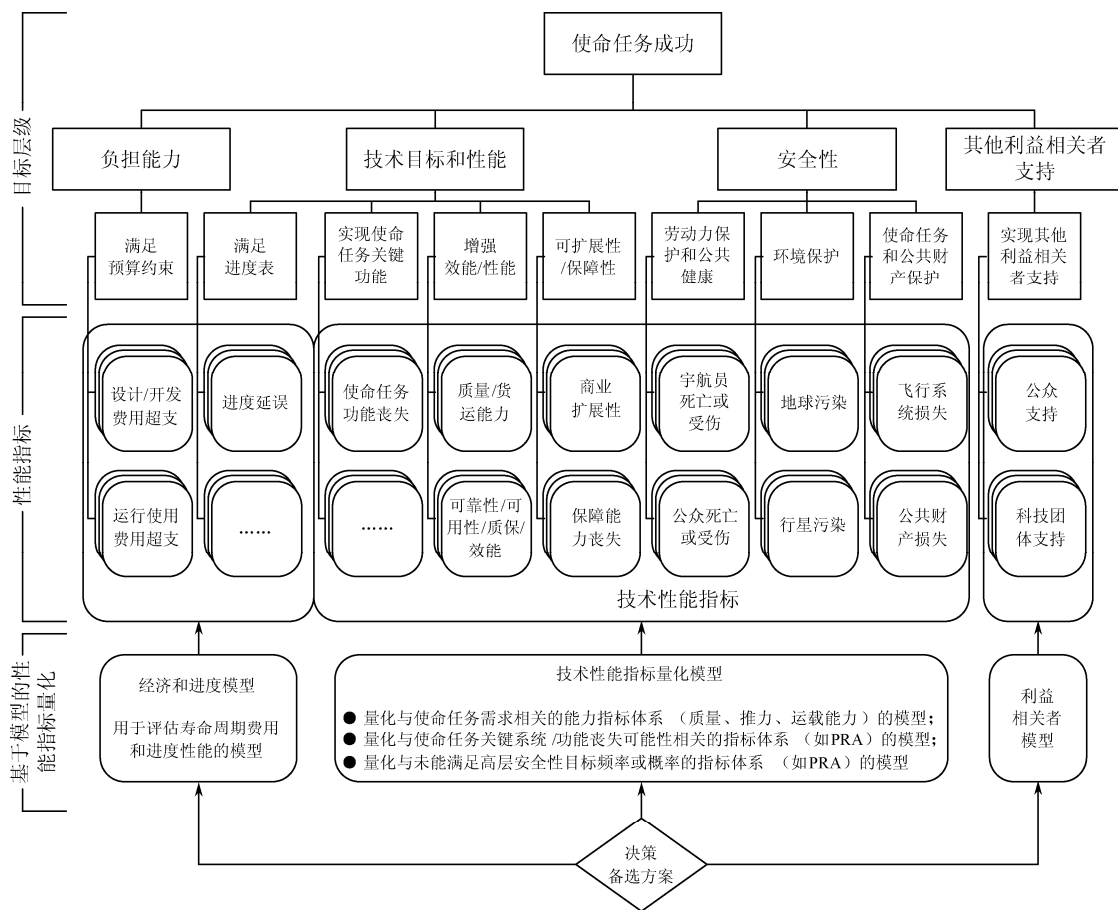


图 6.8-10 目标层次结构示例

第7章 相关专题

本章讨论的主题主要集中于如何增强系统工程流程的执行效率，以及在系统工程实施过程中需要考虑的重要事项。首先阐述如何将系统工程原理应用于 NASA 的合同中，使 NASA 的工程承包商能够履行 NASA 的系统工程流程，从而生产出符合 NASA 要求的产品。在以往的应用中总结的经验教训有助于增强当前项目的效率。在需求开发和系统设计中考考虑保护环境和国家空间资源是非常重要的，一体化设计则能够增强设计流程的效率和效能。

7.1 与合同相关的工程技术

7.1.1 引言、目的和范围

从历史上看，绝大多数成功的 NASA 项目依赖于在 NASA、承包商和第三方之间有效地融合项目管理、系统工程原理和专业技术。这些成功案例的基础是大量协议（如合同、谅解备忘录、合法转让和合作协议等），这些协议可能是 NASA 内各组织之间签订的，也可能是 NASA 与政府机构、政府组织、公司、大学、研究所和实验室等之间签订的。为了简化描述，使用术语“合同”来指代所有类型的协议。

本节重点讨论有关合同签订、合同管理和合同完成的工程技术活动。当然，也讨论采购流程接口，而工程技术团队在合同文件的产生和评估中扮演关键角色。

承包商和第三方团体可以补充（或者是替代）NASA 项目技术团队完成公共技术流程的活动和需求。考虑到承包商可能在系统工程寿命周期的任何阶段发挥作用，NASA 的项目技术团队需要知道如何准备、实施和完成对分派给承包商的技术活动的监督。

7.1.2 采办策略

确定一个项目的采办策略需要那些促成项目审批执行的 NASA 总部各个部门的协作。工程和项目办公室应充分详细地描述采办策略，确定执行采办策略须签订的合同。只有从工程采办策略全局上考虑才能确定项目合同能否签订。

本节考虑的情况是已经决定某个承包商承担项目的部分内容。必须牢记，选择 NASA 自行“制造”产品还是从承包商那里“购买”产品是系统开发中最关键的决策问题之一（参见 5.1 节）。在做出“开发/购买”决策时必须考虑如下问题：

- 所需要的产品是新开发产品还是已有成品？
- NASA 面对潜在的承包商有什么相关经验？
- 风险、费用、进度和性能间的相对重要性如何？
- 是否需要保持自身开发的能力？

一旦确定了需要签订合同来获得系统或服务，项目负责人需要联系外购办公室。合同主管官员将委派合同专家协助梳理涉及 NASA 采购的大量常规需求条款并指导撰写合同文本，确定合同经费，必要时合同专家将请求法律办公室的帮助。

7.1.2.1 制定采办策略

在合同专家和法律专家的协助下，项目负责人首先制定或者选择一个采办策略。采办策略提供业务和技术管理的提纲，用于计划、指导和管理该项目通过合同得到目标产品和服务。

在某些情况下，需要适当调查外部商家以搜集足够的信息来形成采办策略。通过向期望获得未来潜在合同的工业部门或其他团体发出信息咨询调查表可以实现这一点。发放信息咨询调查表是一种获取可能影响采办策略决策的有关技术成熟度、技术挑战、能力、价格和交付细则及其他市场信息的有效途径。

采办策略内容如下：

- 采办目标——需要提供的能力，主要里程碑。
- 采办途径——单步骤或演化（递进）过程，单个或多个供货商/承包商，竞争或唯一商家，经费来源，阶段划分，系统集成，商用现货（COTS）。
- 业务因素考虑——约束（如经费、进度），资产和技术可用性，商业产品与内部技术开发产品之间的适用性对比。
- 产品或服务的采办风险管理——主要风险，与供货商的风险分担。
- 合同类型——基于性能或基于成果水平，固定价格或成本补偿。
- 合同要素——动机，性能参数，确定合同类型的决策依据。
- 产品保障策略——系统交付监督，维护，改进。

技术团队收集数据，推动与上述各项相关的决策过程。技术团队负责发布采办方法，确定资产和技术的可用性、商用产品的适用性，发布系统集成和产品交付细节。相应的，技术团队负责提供如何辨识和评估所需产品采办风险的相关知识，特别是关于合同类型和特殊合同要素部分的知识。

7.1.2.2 采办寿命周期

合同活动是采办寿命周期的一部分，包括合同招商，商户选择，合同监督和合同验收（见图 7.1-1）。采办寿命周期与项目寿命周期的系统工程流程重叠交接。采办计划重点关注需要特殊合同（或购买）时的技术规划（参见 6.1 节）。在图 7.1-1 中，需求开发与系统工程引擎中的技术需求定义流程相关（见图 2.1-1）。接下来的四个阶段——合同招商、商户选择、合同监督和合同验收属于合同活动。交付使用维护表示将采办到的产品转交给负责使用和维护的组织（可能是承包商）的活动。采办管理参照项目管理活动，由采办组织在整个采办寿命周期中实施。

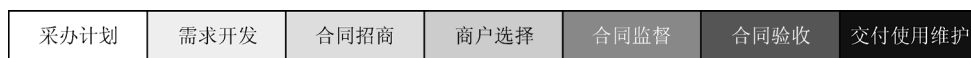


图 7.1-1 采办寿命周期

7.1.2.3 NASA 系统工程职责

技术团队负责整个采办寿命周期的系统工程活动。不管采用什么采办策略，面临什么样

的供货商、承包商和分包商的组合，技术团队对系统工程决策和结果负有重大责任。即使是采办策略要求由技术团队或主承包商或两者的某种结合对不同来源的产品进行系统集成或试验，系统工程活动仍由技术团队负责。

本小节给出将技术流程写入合同时如何进行责任分工的指南。一般来说，项目的技术规划流程、接口管理流程、技术风险管理流程、技术状态管理流程、技术数据管理流程、技术评估流程和决策分析流程由 NASA 团队和承包商在项目寿命周期内共同实施。利益相关者期望定义、技术需求定义、系统逻辑分解、设计方案定义、产品研制实施和集成、产品验证和确认、产品交付和需求管理流程需要根据产品分解层次，由 NASA 团队或承包商实施。

表 7.1-1 给出实施 NPR 7123.1 中确定的 17 项技术流程的指南。前两列是技术流程编号和相关职责的需求陈述。第三列给出如何辨别实施该流程的责任方的一般指南。最后一列给出针对特定项目流程实施的应用实例。该实例描述承包商参与建造空间飞行器的科学任务，NASA 为承包商安排属于政府登记资产（GFP）的设备，最终任务由 NASA 执行。

表 7.1-1 合同的技术流程应用

编 号	NPR 7123.1 技术流程	流程实施责任方	科学使命任务应用实例
1	NASA 中心主任或其代表建立和维护工作分解结构模型中利益相关者期望定义的流程，包含活动、需求、指南和文档	如果利益相关者是承包商，则承包商负有责任，反之亦然	NASA 是使命任务/项目的利益相关者；承包商是空间飞行器电源子系统的主要利益相关者
2	中心主任或其代表建立和维护工作分解结构模型中与利益相关者期望相符的技术需求定义的流程，包含活动、需求、指南和文档	由利益相关者分派需求和职责，如果利益相关者是承包商，则承包商负责提出需求，反之亦然	NASA 提出顶层需求，由承包商提出电源子系统的需求
3	中心主任或其代表建立和维护工作分解结构模型中确认技术需求的逻辑分解的流程，包含活动、需求、指南和文档	根据需求确定，如果需求由承包商提出，则承包商负责实施需求的分解，反之亦然	NASA 实施高层需求分解，承包商实施电源子系统需求分解
4	中心主任或其代表建立和维护满足技术需求的工作分解结构模型中产品设计方案定义的流程，包含活动、需求、指南和文档	根据需求确定，如果需求由承包商提出，则承包商负责实施产品方案设计，反之亦然	NASA 设计使命任务/项目层方案，承包商设计电源子系统方案
5	中心主任或其代表建立和维护工作分解结构模型中通过制造、购买或重用目标产品实现设计方案定义的流程，包含活动、需求、指南和文档	设计后确定，如果设计方案是承包商提出，则承包商负责按设计方案实施产品研制，反之亦然	NASA 完成使命任务/项目层设计产品的实施执行，承包商则完成电源子系统的研制
6	中心主任或其代表建立和维护工作分解结构模型中根据设计方案定义将低层产品集成到目标产品的流程，包含活动、需求、指南和文档	设计后确定，如果设计开发由承包商完成，则承包商负责实施设计单元的集成，反之亦然	NASA 负责集成使命任务/项目层的设计，承包商完成电源系统集成
7	中心主任或其代表建立和维护面向设计方案定义的对由产品实施执行流程或产品集成流程形成的目标产品进行验证的流程，包含活动、需求、指南和文档	产品集成后确定，如果产品由承包商集成，则承包商负责产品的验证，反之亦然	NASA 负责验证使命任务/项目，承包商负责验证电源子系统
8	中心主任或其代表建立和维护面向利益相关者期望的对由产品实施执行流程或产品集成流程形成的目标产品进行确认的流程，包含活动、需求、指南和文档	产品集成后确定，如果产品由承包商集成，则承包商负责产品的确认，反之亦然	NASA 负责确认使命任务/项目，承包商负责确认电源子系统

续表

编 号	NPR 7123.1 技术流程	流程实施责任方	科学使命任务应用实例
9	中心主任或其代表建立和维护将目标产品交付到工作分解结构模型中较高层次客户或用户的流程, 包含活动、需求、指南和文档	产品验证和确认后确定, 如果由承包商验证和确认产品, 则承包商完成产品交付, 反之亦然	NASA 将使任务和项目交付使用, 承包商则向空间飞行器层次交付电源子系统
10	中心主任或其代表建立和维护规划技术研究的流程, 包含活动、需求、指南和文档	假设 NASA 和承包商都进行技术开发工作, 则 NASA 和承包商皆需要规划他们相应的技术研究	NASA 规划与政府登记资产设备及与空间飞行器发射和运行使用相关的技术研究, 开发商规划与电源子系统设计、制造、验证确认、交付使用相关的技术研究
11	中心主任或其代表建立和维护在系统设计过程中定义和确定控制基线的需求管理流程, 包含活动、需求、指南和文档	在流程#2 后确定	
12	中心主任或其代表建立和维护在系统设计过程中定义和生成的接口管理流程, 包含活动、需求、指南和文档	接口应当在接口对应单元的上一层管理	空间飞行器与地面系统的接口由 NASA 管理, 承包商负责管理电源子系统与高度控制子系统的接口
13	中心主任或其代表建立和维护在技术研究中辨识的技术风险管理流程, 包含活动、需求、指南和文档。NPR 8000.4 《NASA 风险管理流程需求》提供定义该流程的文档依据; NPR 8705.5 《NASA 工程项目概率风险评估技术规程》提供辨识和评估技术风险的途径	NASA 和承包商都应该对技术风险进行管理。项目的所有单元都应辨识其风险, 并参与项目风险管理。决定何时以何代价缩减哪项风险, 通常是 NASA 项目管理的内容之一	NASA 项目管理应该制定有承包商参与的项目风险管理方法。整个项目中辨识的影响到电源子系统及更低层次的风险应被辨识并向 NASA 报告, 以便进行可能的缩减
14	中心主任或其代表建立和维护技术状态管理的流程, 包含活动、需求、指南和文档	像风险管理一样, 技术状态管理需要 NASA 与承包商团队在整个项目中共同实施	NASA 项目管理应该制定有承包商参与的技术状态管理方法。承包商内部的技术状态管理必须集成在 NASA 的方法中。技术状态管理需要在全项目实施, 直到电源子系统及更低层
15	中心主任或其代表建立和维护在技术研究中产生的技术数据管理的流程, 包含活动、需求、指南和文档	与风险管理和技术状态管理一样, 技术数据管理需要 NASA 与承包商团队在整个项目共同实施	NASA 项目管理应该制定有承包商参与的技术数据管理方法。承包商内部的技术数据管理必须集成在 NASA 的方法中。技术数据管理需要在整个项目中实施, 直到电源子系统及更低层
16	中心主任或其代表建立和维护对规划的技术研究进展和需求满足度进展的评估流程, 包含活动、需求、指南和文档	进展评估需要 NASA 与承包商团队在整个项目共同实施	NASA 项目管理应该制定有承包商参与的评估项目进展方法。典型的是项目评审计划。承包商内部的评审流程必须集成在 NASA 的方法中。技术评审需要在整个项目中实施, 直到电源子系统及更低层

续表

编 号	NPR 7123.1 技术流程	流程实施责任方	科学使命任务应用实例
17	中心主任或其代表建立和维护技术决策的流程，包含活动、需求、指南和文档	很明显，技术决策由 NASA 与承包商双方人员在整个项目中共同制定。特定类型和特定主题的决策最好由 NASA 或承包商单方决定，这依赖于 NASA 中心建立的流程和项目的类型	在本例中，影响高层需求和使命任务成功的决策由 NASA 制定，而像电源子系统中不影响使命任务成功的低层决策由承包商作出

7.1.3 签订合同前的工作

7.1.3.1 采办计划

在制定系统工程管理计划时，技术团队要基于采办策略制定采办计划并归档。系统工程管理计划涵盖了在签订合同之前、执行合同期间直到完成合同期间技术团队的活动。采办计划中包括招商准备、商户选择、明确合同条款、监督承包商绩效、产品验收、完成合同，以及最终交付。系统工程管理计划关注 NASA 与承包商间的交互，包括 NASA 技术团队参与和监督合同规定的工作。

在项目人工估算时经常被忽略的是技术团队成员参与合同相关工作花费的大量时间。根据采购方式的不同，技术团队的成员可能需要花费 6~12 个月的全工时参与商户选择。合同签订后，技术监督需花费 30%~50% 的精力，而在重要里程碑和关键交付件到达时，需要花费全部精力。切记在多数承包商活动中，NASA 雇员进行的只是补充活动。

技术团队密切参与采办标书的技术文档开发。采办标书包括招商（如申请指南）和支撑文档。招商包括公布给可能的承包商（或应招商）的所有文档。招商文档中的关键技术环节包括任务书、技术规范和数据需求列表。招商文档的其他环节包括申请指南和评价准则。招商支撑文档包括采购进度计划、商户评估计划、政府费用概算和购买要求。部分支撑文档的制定需要技术团队的参与。

合同专家的职责是，根据技术团队的要求，确保招商文件中包含适当的条款。合同专家熟悉联邦采办法规和 NASA 采办法规附则的要求，这两个法规要求以全文或引用形式包含在招商文件的条款中。大部分条款与国家法律、合同管理、财政管理相关。较新的条款强调信息技术安全、数据所有权、知识产权、新技术报告和类似内容。合同专家与联邦采办法规和 NASA 采办法规附则的更新保持一致。随着招商文件中任务书和其他部分逐渐成形，合同专家和技术团队应密切合作，避免出现重复需求。

招 商 文 件

对有关团体发布的招商文件是未来合同的正式表征。招商文件充分详细地表述政府需求（包括条目、条件和指南），并允许可能的承包商（或应招商）提出申请响应。根据工作的重要性及复杂性，可能发布招商草案。在接到申请后，商户评价委员会依照商户评价计划对技术和商务申请进行评价，并向合同负责官员推荐选定的承包商。商户评价委员会由一位技术专家领导，包括其他技术专家和一位合同专家。商户选择过程在合同负责官员签订合同后完成。

最常见的 NASA 招商类型为发布申请指南和商机公示。可以登录 NASA 在线采购资料库获取关于采购和商户选择的详细过程。

7.1.3.2 制定任务书

对承包商的有效监督始于制定任务书。技术团队为所需产品建立任务书需求。任务书包含承包商在产品开发期间必须满足的流程、性能和管理需求。

如图 7.1-2 所示，技术团队在制定任务书时需分析承包商应完成的工作、实现的性能和数据。这个过程是循环反复的过程，并且为合同工作所需的文档制定提供支持，主要步骤见表 7.1-2。

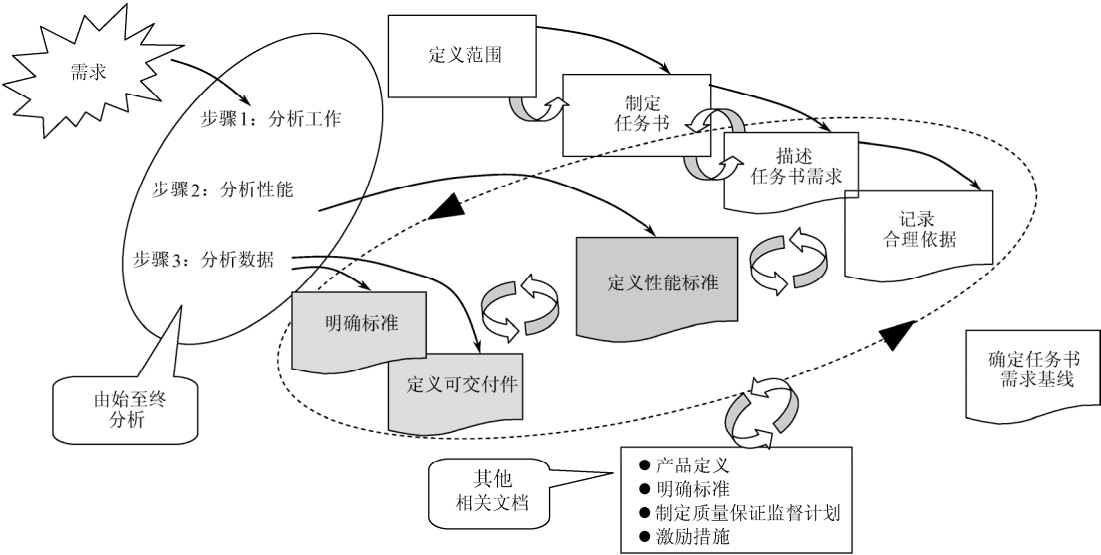


图 7.1-2 合同需求制定过程

表 7.1-2 需求制定流程步骤

步 骤	任 务	细 节
步骤 1： 分析工作	定义范围	在任务书中确定合同内容所属的项目范围，为面对的应招商提供充分的背景信息
	组织制定任务书	根据产品和相关活动（即产品工作分解结构）组织工作
	描述任务书需求	开展下列工作需要包括的活动： ● 开发需求规范中定义的产品； ● 保障、管理和监督产品的开发。 以“承包商需要能够”的形式陈述任务书需求；以“系统需要”的形式陈述产品需求
	归档依据	分别归档任务书中所包括的可能是独特的、不寻常的、有争议的和政治性需求的理由。依据不是招商的一部分
步骤 2： 分析性能	定义性能标准	定义承包商可接受性能指标的构成。标准的通用性能指标需包括成本和进度。承包商绩效评估和交付产品需求满足度评估的指标指南参见《基于性能订约的系统和软件指标》
步骤 3： 分析数据	明确标准	确定用于可交付工作产品（包括计划、报告、规范、图表等）的标准（如 EIA、IEEE、ISO）。用于产品开发和加工的公共标准和章程（如国家电工技术规程、国家消防协会规程、美国机械工程师协会规程）应包含在规范中
	定义交付件	确保每个可交付数据项（如技术数据——需求规范、设计文档，管理数据——计划、指标集报告）的准备有相应任务书与其相应。确保每个产品有相应任务书用于其交付

经过若干次反复迭代，确定任务书需求控制基线，并将其列入技术状态管理（参见 6.5 节）。

附录 P 的任务书清单帮助确保任务书是完整的、一致的、正确的、清晰的、可证实的。必须在任务书中包含的关键事项如下：

- 有最高潜在风险的技术和管理交付件（如系统工程管理计划、开发和交付计划）；需求和结构规范；试验计划、程序和报告；度量指标报告；交货、安装和维护文档。
- 合同中约定或安排的额外奖励不能放入技术里程碑评审。里程碑评审（如系统需求评审、初步设计评审、关键设计评审等）保证关键的和重要的技术评估的进行。这些评审有不能忽略的特定的启动条件。评审应由是否满足启动标准引导，而非由某个特殊的计划驱动。
- 为评估承包商最终交付件进展而需要的电子数据、工作产品和临时交付件的适时访问权。
- 把需求分解给分包商或者其他团队成员的条款。
- 合同数据需求清单中交付件的内容和格式需求。这些需求在通常作为附件的数据需求文档或数据项描述中指定。切记需要可编辑数据交付件。
- 获得对每个学科（如硬件、软件、热学、光学、电学、机械）技术进展可预见的指标。承包商绩效评估和交货产品需求满足度评估的指标指南参见《基于性能订约的系统和软件指标》。
- 为缩减低质量交付件的风险（缺陷、数量错误等），在质量方面的额外奖励，需当心额外奖励可能影响承包商行为。例如，若奖励软件缺陷的早期发现和更正，承包商可能夸大更正次要缺陷的工作而暂缓解决主要缺陷的努力。
- 持续的工程管理，包括定期更新的风险清单、联合风险评审和供货商风险处理。
- 对进展和生产的监控活动（如状况汇报、评审、审核和考察），特别是针对分包商和其他团队的成员。
- 需要满足标准和验证需求的专业工程技术（如可靠性、质量保证、低温学、烟火技术、生物医学、废品管理）。
- 根据签署合同前尚不适用的验证、确认或相近计划在 NASA 和承包商之间确定职责的条款。
- 促使承包商对改变关键流程进行说明的条款。如果一个流程对人员生命安全有影响，承包商在将其变更到另一个流程实施之前，需要得到合同官员的批准。

注：如果在任务书中忽略了某些需要的内容，后期将其加入代价更大。

承包商必须提供一份系统工程管理计划，说明其在需求开发、技术方案定义、设计实现、产品评价、产品交付，以及在技术规划、控制、评估和决策分析中的系统工程方法。最好在招商时就要求一个初步的系统工程管理计划。商户评价委员会可以根据系统工程管理计划评价应招商对需求的理解，以及应招商交付系统的能力。合同签订后，如果在项目系统工程管理计划和承包商系统工程管理计划之间出现影响一体化通用技术流程顺利进行的差别，技术团队可以将其消除。

通常，技术团队有开发系统需求的经验，却很少有制定任务书需求的经验。如果向承包商提出一组复杂的技术需求，却忽略了足够的性能指标和报告需求，便很难监督承包商进展和确定产品和过程质量。明确性能指标和报告需求则能够要求适当的数据和报告供使用需要。

传统上，NASA 合同要求承包商满足 NASA 政策方针、NASA 程序需求、NASA 标准及

相近文档。这些文档几乎没有可以直接用于合同的文字。在大多数情况下，这些文档包含的需求不适用于合同。因此，在技术团队准备像以前多数情况那样做之前，最好是理解需求的内涵及其是否适合合同。应用于合同的需求应当写成适合合同的文本形式。

7.1.3.3 任务订单合同

有时技术团队可以通过现成的任务订单合同模式获得工程产品和服务。技术团队制定任务订单的任务书，并联系合同官员的技术代表发布任务订单。任务订单任务书的准备是经过简化的，因为现成合同中已经明确了执行的控制基线需求。首次使用者需要了解合同范围，以及合同已经覆盖的交付与报告需求、性能指标、激励措施等。任务合同为研究、分析、设计、开发和试验的工程技术服务和技术状态管理、质量保证、维护和使用的保障服务提供（数天或数周代替数月）快速获取能力。一旦任务订单发布，技术团队开展与管理合同绩效和完成合同（后面讨论）相关的应用于任务订单的工程技术活动。

7.1.3.4 监督计划

监督计划定义对承包商工作的监控，与任务书同时开发。技术团队与通常来自 NASA 安全与使命任务保证机构的人员共同准备对合同任务的监督计划。有时使命任务保证由项目的技术专家承担。不论哪种情况，使命任务保证人员应当在项目开始即投入工作。在签订合同之前，监督计划处于系统总体层次，涵盖政府能够感知计划性风险的方法。合同签订后，在当时对计划性风险感知水平下，监督计划则详细描述调查、试验和其他质量相关的监督活动，以保证合同产品的完整。

推荐监督计划包含的条目如下：

- 在 30 天内评审关键交付件以确保监督活动适当启动；
- 实地考察承包商/分包商，监控生产和评估进展；
- 评估承包商系统工程流程的绩效。

开发任务书同时起草监督计划，更多地将任务书中的关键需求体现在监督计划中。例如，为了让技术团队能够对分包商进行实地考察监控生产，任务书中必须包含允许现场视察的需求，以及承包商应将那些直接影响分包商的需求分解到位的需求。

7.1.3.5 撰写项目申请指南和评价标准

一旦技术团队制订了任务书、政府费用估算、初步监督计划和更新的系统工程管理计划，即可开始招商。招商文件的撰写者必须了解评价项目申请书所需的信息，并撰写获得具体所需信息的指南。在典型的商户选择中，商户选择委员会评价每个应招商对需求、管理方法和费用的理解及其相关经验和以往绩效。这是商业和技术申请书中需要的内容（本节仅讨论技术申请）。招商文件同时给出商户评价委员会使用的评价标准。本节内容与申请书指南中要求的条目一一对应。

指南应清晰正确陈述，其目的是得到足够的信息作为评价的基础。面临的挑战是应该提供给应招商多少信息。如果指南中规则太多，则申请书看起来会非常相似。注意不要“把运动场做得太平整”，否则很难区分应招商的水平。因为申请书的技术水平与非技术事项（如费用）有相似的重要性，技术团队必须明智地选择识别方法以便于商户选择。

商户评价委员会评价非技术（商业）和技术内容。可以评价技术内容自身，也可以在其

他技术和非技术内容的影响下进行评价。表 7.1-3 列举了要求应招商提供的技术内容及其相关的评价准则。

表 7.1-3 申请书评价标准

内 容	标 准
承包商的初步系统工程管理计划	在确定资源、流程、控制的条件下，计划可以完成的程度。着眼于完备性（对任务书需求的覆盖程度）、内部一致性、与其他申请书内容的一致性。系统工程管理计划应该涵盖满足产品需求的所有资源和学科
流程描述，包括分包商（或团队成员）的流程	流程的绩效，承包商与分包商流程的兼容性（如职责、决策、问题解决方案和报告）
曾完成相关工作的档案（文档）。这类文档描述应招商根据合同能够提供的工作产品可能的质量水平。档案为执行系统工程流程能力（或缺失）提供证据	完整的存档、指定内容存档的一致性，交叉项目存档的一致性，与标准的一致性
工程技术方法和工具	方法和工具的有效性
流程和产品度量指标	对应招商度量其流程和产品质量的优劣判断
分包合同管理计划（可能是承包商系统工程管理计划的一部分）	对分包商监督和控制的有效性，风险管理和技术状态管理的集成和分解
分段实施计划（可能是承包商系统工程管理计划的一部分）	在给定资源和工作负载条件下，计划执行的情况

商户评价委员会

商户评价委员会需要一个或多个技术团队成员的参与，他们遵循 NASA 总部和中心的商户选择流程参与对申请书的评价。由于商户选择非常重要，采购办公室应与商户评价委员会密切合作，确保商户选择过程的顺利进行。商户评价专家组制定商户评价计划，描述评价因子和对应招商申请书的评价方法。与产品寿命周期早期系统工程师的决策不同，商户选择决策必须依据保证选择过程公正性的规则精心管理。

评价需考虑事项

在评价申请书时需要重点考虑的内容如下：

- 评价可能导致使命任务失败的那些学科（如硬件、软件、热学、光学、电学、机械学）能力时给予适当的权重。
- 合同签订前对使命任务成功至关重要的生产/试验设施进行实地考察。
- 区分“投机者”（能写好的申请书）和“竞标者”（能良好地组织执行）。特别要注意流程描述如何与相关经验和已有成就匹配。好的申请书预示未来好的性能，低质量的申请书通常预示未来工作产品和目标产品的较低质量。
- 按照评价准则评估承包商的系统工程管理计划及申请书中的其他条目，评价准则包括质量特性（如完整性、清晰性、一致性、可验证和可追溯性）。

作为技术规划流程的一部分，技术团队进行的成本估算支持评价应招商的费用申请，帮助商户评价委员会确定应招商技术申请书的现实性（参见 6.1 节）。商户评价委员会可以确定“申请书估算的分项成本对于需开展的工作是否现实，是否反映了对需求的清晰理解；与应招商技术申请书中描述的性能和材料的计算方法是否一致”。

7.1.3.6 现货产品选择

若现货产品作为技术解决方案的一部分出现在申请书中，则需运用决策分析流程对特定产品的选择进行评价并归档是极为重要的。回避这项工作或忽略对评价结果的完整归档可能导致 NASA 在遇到供货商抗议事件时处于不利境地。

7.1.3.7 采办特有的风险

表 7.1-4 列举了一些采办所独有的风险，以及从工程角度对这些风险进行管理的方法。切记，这些风险的处理方式通常要写入合同中。

表 7.1-4 采办风险

风 险	缩 减 方 案
供应商在交货前破产	商户选择流程是最有力的武器。选择一个有良好记录、资金牢固、员工稳定的供应商。作为最终补救，政府可以征用工作现场的材料、设备和设施，以备 NASA 自己完成或通过另一个合同完成工作的需要
供应商被其他有不同政策的企业收购	比较收购发生之前和之后政策的不同。若有关键性的不同，则需咨询采购和法律办公室。与供应商会谈并确定原政策是否会在无附加费用情况下被继续遵守。如果供应商不愿意，则按照法律顾问的意见办理
交付件包含待开发软件	在技术团队中选入一名有经验的软件负责人。监测承包商遵循软件开发流程的程度。在技术交流会议上讨论软件进展、问题和质量
交付件包含现货产品（特别是软件）	了解产品质量。 查看试验结果。如果试验结果显示需要进行大量更正缺陷的工作，则用户可能进一步发现更多的问题。 检查问题报告，这些报告显示软件发布后用户是否仍在发现新的问题。 评价用户文档。 查看产品售后服务
产品依赖于建模和仿真结果	建立仿真结果的可信度和不确定度。确定用于模型或仿真的验证和确认活动的深度和广度。了解作为模型或仿真基础的软件质量。 更多信息请参考 NASA-STD-(I)-7009 《模型与仿真标准》
在交付所有产品前预算发生变更（合同没有注明中间交付件）	选择包括如下： <ul style="list-style-type: none"> 为了获得关键产品，取消合同中不必要的产品或服务。 放宽进度限制以缩减费用。 按“现有水平”接受交付件。 为避免这种情况，合同中应列入对数据、工作产品、中间交付件的电子访问权，以针对任务书中的最终交付件评估承包商的进展
承包商是专业供应商，缺乏特定工程学科的经验。例如，承包商生产低温系统，使用另一个供应商的温度监控报警软件，但其自身没有软件专家	如同前文讨论的现货产品风险缩减。如果合同要求交付改进的现货产品或是客户产品，那么在任务书中应包含涵盖下列内容的条款： <ul style="list-style-type: none"> 供应商（产品质量保证书之外）的售后服务应包括次级供货商的售后服务。 版本升级/替换计划。 监督次级供应商。 如果产品不贵重，简单购买备品可能比加入监控需求的费效比更高

可能还有表 7.1-4 没有列出的采办风险。所有采办风险必须像项目中其他风险那样运用

持续风险管理流程辨识和控制。如果确实需要，项目也可以选择分离出采办风险作为风险列表的子集，运用基于风险的采办管理流程对其进行控制。

技术团队在完成所有签订合同前的工作时，将更新系统工程管理计划、政府成本估算、任务书及初步监督计划。一旦合同签订，技术团队开始技术监督工作。

7.1.4 履行合同期间

7.1.4.1 进行技术监督

对承包商的活动和/或文档进行监督是为了履行财政职责，确保人员安全和使命任务成功，并确定合同额外工作的奖励费（或不合格工作的罚金）。在合同签订之前及合同之外，签一个较小的正式协议，使政府能够得到进行权衡和工程评价所需的信息。合同签订后，有必要监督承包商遵从合同需求的程度（对监督需求的进一步了解，参见 NPR 8735.2《NASA 合同中政府质量保证功能管理》）。

在合同官员授权下，NASA 技术团队执行 NASA 系统工程管理计划中制定的技术监督工作。技术团队评估技术工作生产效率、评价产品质量并对承包商进行技术评审（参见技术评估流程）。下文讨论部分主要活动。

- **建立 NASA 与承包商的技术联系：**在合同会谈开始时，设定合同执行过程中对技术成就的期望。突出显示合同任务书中最为重要的需求。讨论反映技术需求的需交付产品和工作的质量。在技术评审形式和如何解决争端方面达成共识。
- **召开技术交流会议：**在合同早期开始，并定期与承包商（及分包商）举行会议，确认承包商对产品需求、运行使用构想有完整正确的理解。建立 NASA 与承包商的日常技术交流机制。
- **控制和管理需求：**新生的和衍生的需求几乎不可避免会对项目产生影响。当需要变更时，技术团队需要控制和管理 NASA 或者承包商提出的需求变更和附加需求（见 6.2 节）。要与变更影响到的所有项目参与方进行沟通。任何会影响合同费用、进度、性能的需求变更，必须通过正式合同变更形式传达给承包商。此工作需向合同官员的技术代表进行咨询。
- **评价系统工程流程：**评价所定义的系统工程流程的有效性。对流程进行审核和评审。辨识流程的不足之处，为流程改进提供帮助。
- **评估工作产品：**在系统工程工作中评价中间计划、报告、规范、图纸、技术规程、流程和相近的档案。
- **监督承包商绩效的核心指标：**在规定的流程和产品指标基础上监督承包商的扩展绩效指标（参见 6.7 节关于技术性能指标的论述）。这些指标依赖于可接受的产品质量。例如，“设计图纸完成 50%”在所完成工作中多数有缺陷（如不正确、不完整、不一致）的情况下是有误导的。修正图纸的工作量影响成本和进度。检查承包商在产品检验和评审上投入时间的报告是有用的。
- **进行技术评审：**通过技术评审来评估承包商在满足需求方面的进展和绩效（参见 6.7 节）。
- **验证和确认产品：**在产品交付并与其他系统产品集成前验证和确认其功能和性能。确保产品能够用于系统集成或进一步开发，产品的验证和确认要尽早实施（参见 5.3 与 5.4 节）。

7.1.4.2 评价工作产品

工作产品和交付件有相同的属性，可以用来评估质量。此外，工作产品和交付件之间的联系也可以用来评估质量。下面列举部分确定工作产品质量的关键属性：

- 满足内容和形式需求；
- 易于理解；
- 完整；
- 一致（内部和外部），包括术语（整个文件中对同一事物的称谓）一致；
- 可追溯。

表 7.1-5 列举了部分典型的承包商工作产品，以及可以作为评价标准的涉及其他文档的关键属性。

表 7.1-5 典型的工作产品文件

成 果	评 价 标 准
系统工程管理计划	描述任务书中要求活动和产品。 描述任务书中每项活动和每件产品是如何实现的，否则系统工程管理计划不完整
软件管理/开发计划	与系统工程管理计划和相关项目计划保持一致。 描述任务书中每项软件相关的活动和产品是如何实现的。 开发方法是可行的
系统设计	涵盖技术需求和运行使用构想。 系统设计是可实现的
软件设计	涵盖技术需求和运行使用构想 与硬件设计保持一致。 软件设计是可实现的
安装计划	涵盖任务书要求的所有用户场所的安装活动。 提出合理的方案。 表明与系统工程管理计划和相关项目计划的一致性
试验计划	涵盖任务书中资质需求。 覆盖技术需求。 方案可行
试验技术规程	试验大纲针对技术需求是可追溯的
交付计划	描述任务书中要求的所有交付活动。 表明与系统工程管理计划和相关项目计划的一致性
用户文档	（根据文档）向对象读者充分而适当地描述安装、操作、维护
图纸和文档（一般）	遵从任务书中制定的需求内容和格式

7.1.4.3 关于合同-分包合同安排的问题

在理想情况下，承包商管理其分包商，每个分包合同包含所有的现实需求，资源应是适当的。在现实世界中，技术团队需要面对受利益驱动的承包商和分包商、含有缺失和错误需求的合同（分包合同），以及比预期快的资源消耗。这些因素和其他因素导致或影响分包合同中的两个关键问题：

- 对分包商的监督受限或者完全没有监督；
- 对分包商数据的访问权受限或无权访问。

这些问题在遇到二级（低级）分包商时更严重。表 7.1-6 讨论这些问题并且给出可能的解决方法。

表 7.1-6 合同-分包合同问题

问 题	解 决 方 法
因为合同中缺少相关需求，对分包商监督受限	技术团队向合同官员提交任务书需求，合同官员将需求加入合同中，并针对合同变更根据 NASA 的额外经费与承包商谈判。承包商将需求加入分包合同并与分包商就变更进行谈判。如果技术团队明确要求监督，则任务书应当指出承包商、分包商和团队成员需要做什么和提供什么
因为需求未从承包商分解到分包商，对分包商监督受限	承包商有责任满足合同要求。如果合同中包含将需求分配给分包商的条款，则技术团队可以请求合同官员指令承包商执行该条款。承包商可能要向分包商增加需求并商谈经费变更。如果 NASA 制定的是成本补偿合同，则承包商应当向 NASA 提供所发生的任何附加费用的账单。如果 NASA 制定的是固定价格合同，则承包商要么自己负担额外的费用，要么重新与 NASA 谈判费用变更。若合同未明确包含需求分配条款，承包商有责任对分包商进行监督
因为需求未从分包商分解到二级分包商，对二级分包商监督受限	与前一种情况类似，但稍复杂。假设承包商将需求分解到了分包商，然而分包商没有将其分解到二级分包商。如果分包合同包含分解需求到二级分包商的条款，则技术团队可以请求合同官员指令承包商确保分包商执行其对二级分包商的需求分解。 如果分包合同没有明确包含需求分解条款，则由分包商负责对低级分包商进行监督
因为合同中未要求提供数据，对分包商的数据访问权受限或者无权访问	技术团队向合同官员提交任务书需求，合同官员将需求加入合同中，并针对合同变更根据 NASA 的额外经费与承包商谈判。承包商将需求加入分包合同并与分包商就变更进行谈判。如果技术团队明确要求访问分包商的数据，则任务书中应指明承包商、分包商和团队成员需要做什么和提供什么
因为分包合同中未要求提供数据，对分包商的数据访问权受限或者无权访问	承包商有责任获取数据（和数据访问权）以满足合同条件，包括获取来自分包商的数据。如果技术团队需要直接访问分包商的数据，可以参照上款情况在合同中增加相关条款，承包商也在分包合同中增加相应需求

除了表 7.1-6 中的情况，出现其他情况也是可能的。解决方法可能包括缩小合同和交付件范围来抵消费用的增加，或者共享信息技术以获得数据。即使是在（分包）合同中适当分解需求的情况下，也可能需要通过法律诉讼迫使承包商（分包商）满足（分包）合同要求。

在执行合同期间，需要生成完善的监督计划、细致的会议记录、需求变更通知和合同变更通知。需要评估流程、评价交付件和工作产品，并评审结果。

7.1.5 合同完成

随着合同要求的产品、服务、系统及其支撑产品和系统的交付，合同完成。除了产品之外，同期的技术文档、操作指南和用户手册也需要交付。

7.1.5.1 最终交付件的验收

在合同期间，技术团队评审和接收在合同数据需求列表和产品交付进度计划中标定的工作产品和中间交付件。技术团队还参与交付件确认验收的里程碑评审。在合同结束时，技术团队确保每个技术交付件能够获得且满足验收标准。

技术团队依照合同数据需求和产品交付进度计划记录交付件验收过程。这些文档作为验收的系统和服​​务存档。尽管很少碰到拒绝或者遗漏，但技术团队要在这种情况下发挥作用。良好的数据管理和技术状态管理经验对此有益。

验收标准如下：

- 产品确认和验证顺利完成。技术团队执行或监督产品的验证和确认、产品集成到系统集成的验证和确认，以及系统的验证和确认。
- 技术数据资料是最新的（同期交付的）和完整的。
- 提交的合格证明、备件、质保书等是完备的。
- 提交的软件产品、许可证、数据版权、技术知识产权等是完整的。
- 合同条款要求的技术文档（如相关新技术的报告）是完整的。

NASA 工作人员和相关设施做好接收目标产品准备是重要的。需要准备好的关键内容如下：

- 一份保障和交付产品运行使用的计划；
- 人员培训；
- 技术状态管理系统正常；
- 故障发现、修理、维护的责任分配。

7.1.5.2 交付管理

签订合同之前，作为采办策略的一部分应制定产品保障策略。产品保障策略概要描述与集成、使用、维护、改进、退役和处置相关的初步概念。签订合同后，在系统工程管理计划中确定顶层交付计划，该计划扩展产品保障策略。产品/系统交付的相关细节在随后的一份或者多份交付计划中形成。交付计划的要素已在 5.5 节中讨论。

交付计划必须明确指出（NASA 或者承包商）每个行动的职责。在合同任务书中必须含有相应需求，注明承包商承担交付计划规定的责任（一般以费用补偿的形式）。

通常 NASA（或 NASA 联合主承包商）是项目的系统集成者。在此情况下，多个承包商（或分包商）各自负责相应的交付计划。NASA 负责开发和管理将每个交付计划产品合并的系统集成计划。数月或数年前写入任务书的条款能够保证产品和系统从承包商那里顺利移交到 NASA。

7.1.5.3 使用和保障

系统的成功使用和保障，包括维护和改进，取决于经过利益相关者同意的清晰的交付准则。技术团队参与交付活动，为客户提供持续支持，特别是含有延续合同时。在执行现有合同时，技术团队与承包商召开正式的交付会议。相反，参与交付的可能是不同合同（如修订合同或新合同）约定的同一个承包商，或是不同合同约定的非开发者的其他承包商。

执行现有合同的最大好处是利益相关者熟悉承包商，承包商了解产品和系统。要确保承包商和其他关键利益相关者理解合同的服务条款（需求）。交付会议可能导致合同的修订，以修改或取消数年后已经被合同变更影响的需求。

寻求使用不同合同保留开发承包商是有益的。尽管这需要时间和资源来形成合同，但可以使 NASA 仅根据使用和保障需求来评估承包商和应招商的能力。现任的承包商拥有产品和系统开发知识的人员，而服务商专职于优化服务的成本和有效性。最终，现任者可能因关注

当前（而非若干年前）需求的合同被保留，否则新选的服务商需要为了解如何使用和维护系统努力工作。如果使用延续合同，需向采购办公室咨询，并采取确定开发合同相同的步骤。假设签订延续合同与签订开发合同所需日期相当，同时需要考虑现任者在没有竞争的环境下可能丧失积极性。

在制定任务书时，关于延续合同需要考虑到的若干事项如下：

- 工作人员资质证明；
- 使用的调度、排班和人员组织水平；
- 维修工作剖面（如预防、预测、故障）；
- 维护和改进时机（如进度，周期）；
- 类似工作的历史数据；
- 基于绩效的工作。

使用和保障表明了从产品交付到服务交付的转变。

服务合同关注承包商提供服务活动的的能力，而不是开发产品的能力。因此，绩效标准反映在客户满意度和服务效率，例如：

- 客户满意率；
- 服务效率；
- 对客户需求的响应时间；
- 可用性（如系统可用性、网站可用性、设施可用性）；
- 进行维修活动的时间；
- 计划的和实际的人工组织水平；
- 计划的和实际的服务成本；
- 每次服务活动的工时和费用；
- 每次服务活动工时和费用降低的百分比。

承包商能力评估标准的更多实例，参见《基于性能订约的系统和软件指标》。

7.1.5.4 退役及处置

合同中需要提出安全有效的系统和产品退役处置方法，以及需要的专用的保障系统、设施和训练有素的人员，特别是在含有危险物品时。在制定需求策略时应考虑这些因素，并且在进入详细设计阶段前确定。同时确定产品寿命周期中需要合同的数量。

在制定任务书需求时，关于退役及处置方面需要考虑的事项如下：

- 掌控和处置在制造和组装产品过程中产生的废弃物；
- 重复循环利用资源以减少材料的废弃和转化；
- 掌控和处理产品使用时用到的材料；
- 寿命周期结束时产品的退役和处置；
- 产品、废弃物和多余材料退役和处置所需的费用和进度；
- 产品退役和处置的度量指标。
- 评估承包商绩效的指标（参见《基于性能订约的系统和软件指标》）。

关于处置的相关指导，参见《系统工程手册：系统工程从业者“做什么”指导书》。

7.1.5.5 承包商绩效的最终评价

在准备结束合同时，技术团队向采购办公室提交关于承包商最终绩效评价的报告。尽管技术团队定期评价承包商能力，但最终评价连续记录了执行合同过程中绩效好和绩效差的过程。评价结果保留在数据库中，作为未来商户选择过程中的相关经验和以往绩效参考依据。

这个监督阶段完成于现有合同的结束或修订、后续合同的签订及可用系统交付。监督活动在后续合同中继续。

7.2 一体化设计平台

7.2.1 引言

并行工程和一体化设计是集成产品开发的系统方法，它强调对利益相关者期望的响应，以及团队合作、信任和共享价值的体现。并行工程的目标是通过活动 and 流程的良好集成缩短产品开发周期。并行是减少设计时间的首要概念，而并行工程则成为其焦点。设计中不同部分的并行工作，通过团队间为形成一致意见和决定的简短交流而达成同步。并行工程已成为被广泛接受的概念，被看做处理顺序工程流程的上佳选择。

本节说明并行工程和一体化设计在 NASA “并行工程增长能力”（CACE）环境中的具体应用。CACE 由四个基本组件组成：人员、流程、工具和平台。典型 CACE 环境包括与利益相关者团队共同工作的现场领导小组和多学科核心工程技术团队，该项工作遵循良好定义的流程，使用专用于协同和并行工程的具备特殊工具的平台。工程技术与协同工具通过该平台的集成基础结构相连接。这些团队在技术密集的物理环境中同步进行短期工作，以完成一个设备或任务的设计。CACE 常用于设计空间工具和有效载荷，或是相关任务，如轨道配置、航天器、着陆车、漫游车、探测器和发射器等硬件，以及数据系统和地面通信系统、其他地面系统和使命任务运行操作，但是 CACE 过程不用于严格的工具设计和（或）任务概念设计。

多数 NASA 中心拥有 CACE 平台。NASA 的 CACE 建立在人员/流程/工具/平台的基础上，能够在—个并发、协同、快速设计的环境中加速高质量工程设计概念的形成（见图 7.2-1）。

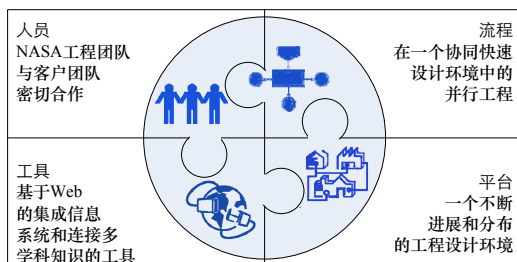


图 7.2-1 CACE 人员/流程/工具/平台范式

尽管 NASA 的 CACE 基于公共的设计思想和特性，但在许多领域 CACE 的实现各不相同。这些差异包括具体工程技术、信息基础结构、知识库、领域专业知识、工程技术人员组织、管理和工程工具、设备化类型、CACE 团队内部的角色和责任、CACE 和利益相关者团队的责任划分、活动执行策略和活动时间。CACE 主要用于寿命周期的早期阶段，如规划和论证阶段，CACE 流程在项目全寿命周期中同样表现出适用性。

7.2.2 CACE 概述及其重要性

CACE 设计技术是专门用于生成快速构造概念、结构和需求清晰表达的有效方法。

CACE 方法能为工程师和利益相关者之间的头脑风暴和跳跃思维提供底层技术支持，这样逐步形成一个高质量的反映客户需要的产品。协同设计范式的成功之处在于能够大幅减少决策时间。而在非 CACE 环境中，问题、议题或争议可能要数天才能解决。如果要改变设计或者重新评估需求，则保证所有工程技术团队成员获得信息或安排利益相关者团队讨论潜在的需求变更可能需要花费大量时间。这些延迟引出初步评价后可能发生的另一轮问题和争议，以及设计和需求的变更，这又进一步增加延迟。

CACE 的工具、数据和支撑信息的技术基础结构提供了技术团队可以立即使用的集成支撑环境。该环境集成了必要的技巧和经验用于同步完成设计。在协同环境下，设计变更发生时，问题可以得到迅速解决，主要参与者可以与利益相关者团队和其他设计团队成员共同开发假设和方案，并迅速使全体团队适应。协作能够激发工程师的创造力，帮助他们结束争议，迅速统一认识。1990 年代中期以来，CACE 方法已成功应用于若干 NASA 中心及商业公司，与传统方法相比极大地缩短了设计时间和费用。

CACE 的利益相关者有 NASA 工程和项目、科学家、技术专家和政府部门（民用或军用）、联邦实验室和大学。CACE 的产品和服务如下：

- 依据 NASA 中心发布的科学指南建立使命任务概念；
- 全过程设计，包括系统/子系统概念、需求和权衡；
- 聚焦于评估特定架构的子单元和折中权衡；
- 对客户提交的报告、概念和成本进行独立评估；
- 路线图支持；
- 技术和风险评估。

一体化设计越来越多地被接受，协同工程设计应用也从一个或多个中心参与的位于同一地点的活动，扩展到地理上分布的若干 NASA 中心有限范围的参与，再到有许多采用广泛而复杂架构的 NASA 一体化设计团队参与的真正的 NASA 一体应用（OneNASA）。

使用地理上分布的 CACE 团队，可以获取 NASA 中的最佳技术和能力，从而得到低风险和创造性的解决方案，这是一个强有力的工程技术方法。考虑到各个 CACE 平台的不同及各个 NASA 中心文化的不同，地理上分布的流程应用必须建立在 CACE 的公共元素上。

7.2.3 CACE 目标和益处

NASA 建立早期 CACE 环境的驱动因素是提高系统工程的效率和效能。特别是早期 CACE 环境要满足的需求如下：

- 利用更短时间和更少费用生成更多概念设计方案；
- 在专用平台中选用明确的工具创造可重用的流程；
- 开发一个供将来使用的任务需求和设计数据库；
- 从有经验的专业工程师中训练任务多面手；
- 在整个组织中灌输更广泛的系统工程思想。

对于 NASA 来说额外得到的长远好处如下：

- 核心竞争力的保障（如发展系统工程师，培养和拓展专业工程师，训练环境等）；
- 使客户群体加深对全过程问题和面向设计的需求含义的感受；
- 用于改进工具和过程的试验床；
- 形成合作伙伴关系的环境；
- 技术发展和路线图支持；
- 质量提高和概念设计的一致性；
- 在 NASA 组织间保证合作而非竞争关系的 OneNASA 环境。

7.2.4 CACE 人员组织

管理或领导团队、多学科工程团队、利益相关者团队和设施保障团队，都是达成成功 CACE 活动的重要因素。

CACE 团队组成包括代表不同学科和专业工程技术领域的工程师队伍，首席系统工程师和一个团队领导或鼓动者。根据需要，核心工程技术团队可以补充专业人员和/或非标准的工程技师以满足利益相关者的特殊需求。这些补充的工程能力可以来自中心内部或外部。团队领导负责协调和推动 CACE 活动，与利益相关者交流以确保其要求能够充分获取和表达。工程师拥有其相关领域知识的技术和软件工具，并与团队领导、其他工程师和利益相关者团队交流，研究解决方案的可行性，并对具体子系统进行设计。

CACE 执行负责人作为中心的代表和管理者，维护 CACE 运行能力，与潜在客户进行初步协调，最终交付 CACE 产品，并且使 CACE 环境的流程和产品持续改进及演化发展，以保证其始终贴近客户群。

CACE 设施保障团队负责维护和开发信息基础结构，以支持 CACE 活动。

7.2.5 CACE 流程

CACE 流程始于客户请求 CACE 管理的支持。CACE 的管理工作确保客户需求在团队的能力和可用范围内，且由团队领导组织多学科工程技术团队并领导工程师与客户团队紧密协作。下面各小节简要描述 CACE 活动的三个主要阶段：（1）计划和准备；（2）活动实施执行；（3）活动总结。

7.2.5.1 计划和准备

客户需求得到认可且团队领导选定后，安排一个计划会议。参加计划会议的主要专家可能包括 CACE 负责人、团队领导、系统工程师，以及来自客户/利益相关者方面的代表。并行设计环节的成功计划、准备和执行必须包括与客户/利益相关者团队的交流及他们在整个过程中的主动参与。考虑的问题方面包括确定活动范围、进度和费用；待交付产品类型的总体协议；成功准则和指标。计划会议达成的协议形成文档，并分发供评审和评议。

计划和准备阶段的产品有客户/利益相关者团队、CACE 团队或两者联合要求的活动，包括定义目标、需求、交付件、预算估算和进度建议。在某些情况下，需要安排后续的协调会议，与会者包括 CACE 团队领导、系统工程师、其他团队成员、客户/利益相关者方面的代表。

会议成员的确定基于已经辨识为活动的动因和任何被认为在实际设计活动开始前需要完成的工作。

在计划和准备阶段，需要对利益相关者提供的数据、目标和活动计划进行评审并最终确定活动范围。每个利益相关者和设计团队具体完成的活动要通过会议讨论决定。例如，对于一个任务设计研究的计划，客户通过定义度量目标和设备规格辨识使命任务目标，并在可能情况下辨识顶层需求。CACE 工程团队的分队需要在实际研究开始之前完成在规划会议上确定的预先研究工作（如运载火箭飞行轨道分析；推进和导航需求；再入、下降和着陆任务剖面；光学分析；机械设计等），以加速活动实施阶段的并行工程过程。这个阶段的分析水平与很多因素相关，包括未来设计的成熟度、工程活动规定的目的和目标、工程师的可用性和 CACE 的进度安排。

7.2.5.2 活动实施执行

典型活动或研究始于客户在适当的情况下向整个团队提供整体使命任务构想和设备构想。客户/利益相关者提供的信息还包括团队目标、科学和技术目标、有效载荷的初始需求、空间飞行器和使命任务设计、部件或功能供应商的任务分解、最大挑战和担心，以及近似的使命任务时限。这些信息通常以电子格式供工程技术团队访问，由客户/利益相关者的代表在高层提交。在提交过程中，每个分系统工程师关注全系统设计中与其分系统相关的部分。系统工程师将高层系统需求放入电子表格和/或数据库，用于在整个过程中跟踪工程变更。这些源数据可以根据需要显示，保证团队成员同步使用，以及客户/利益相关者感知工程最新进展。

工程技术分析反复迭代进行，CACE 团队领导和系统工程师在引导该流程的进行中起重要作用。坚持这个流程就能快速发现问题，并达成权衡决策和需求重新定义的共识。客户团队主动参与协同过程（如权衡研究、需求松弛、定义优先级），有助于快速开发可接受的产品。

当部分团队需要讨论特殊的权衡研究时，经常出现中断环节或私下会谈。每个分系统都有一个用于描述其设计的关键参数集。由于不同分系统间的依赖性，每个学科的工程师需要了解与其他分系统相关的参数值。这些参数通过 CACE 信息基础结构共享。各个分系统间经常有相互冲突或竞争的目标。一旦问题发生，各个分系统专家立即组织由团队系统工程师确定和领导的权衡研究。多数团队成员之间的交流通过面对面会谈，或通过视频及远程会议进行。需要的话，可以咨询其他相关主题的专家。在 CACE 环境中，需要密切交互的分系统应非常接近地集中，以便于专家之间的交流。

团队通过反复迭代不断明确需求，各分系统专家在进度安排允许范围内，细化或修订设计选项。这个流程在得到可接受的解决方案前不断持续。也有可能在进度表安排的活动结束之前，不能通过反复迭代得出可接受的方案。在这种情况下，将可用的反复讨论结果写成文档，形成可交付产品的基础。

在每一步迭代中，将发生如下一些活动，有时顺序发生，有时并行发生。分系统中有关科学、设备、使命任务设计和地面系统方面的专家协同工作，为待解决使命任务问题定义科学数据策略。远程通信、地面系统、指令和数据处理方面的专家协同开发数据返回策略。姿态控制系统、电力、推进、热学和结构方面的专家为对航天器设计进行反复讨论，而技术状态专家则在准备初步设想。系统工程师与所有学科领域工程师进行交互，确保各个分系统设计及既定的系统结构相匹配。每个分系统专家提交设计和费用信息，费用专家估算使命任务的全部成本。

尽管一体化协同设计活动通常只需花费数天或数周，目标产品在研究完成后数周内得到，但利用并行、协同环境进行较长时间更加详细的研究比在 CACE 中花费较短时间的实践能得到更多的好处。

7.2.5.3 活动总结

CACE 研究结束后，产品交付给客户。在某些 CACE 环境中，利用很小的额外资源完成产品的总结：工程师通过加入强调问题已清理的附加信息来响应客户/利益相关者的反馈。在其他 CACE 环境中，形成最终的报告并与客户/利益相关者共同评审，以保证其期望已经充分说明，这可能要花费可观的时间。

某些 CACE 环境对其总结活动进行标准化，强调客户/利益相关者的反馈，在不同的工作范围开发结构化的统一形式的产品。

作为活动延续的一部分，产品是否满足需求，以及是否有改进建议，这些客户/利益相关者的反馈需要进行处理。这些反馈将作为 CACE 环境中持续改进过程的部分因素。

7.2.6 CACE 工程的工具和技巧

CACE 环境的工程技术工具和技巧在若干技术方面变化（如逼真度水平、集成程度、通用的商业应用、对应客户工具、对应客户化知识库的 Excel 电子表格、参数化设计和/或工程分析的维度）。例如，机械设计工具涵盖了从白板讨论，到便签转换，到计算机辅助设计，再到 3D 快速设计原型。

确定使用哪种工具适合某一活动的重要因素包括活动的目的和持续时间、工程师的熟悉程度和偏爱、期望的产品、本地文化和工程环境的演变。选择 CACE 工具和工程技术要考虑的因素还包括对 CACE 环境和过程的适应性、兼容性，以及 CACE 活动对客户的使用灵活性和使用灵活性。

工程技术工具可能集成在 CACE 基础结构中，由保障工程人员逐步提供，也可能仅仅在系列活动中适当应用。如果需要，可以在 CACE 环境外部进行 CACE 工作范围外的辅助工程分析，并且可以作为参考引入到 CACE 产品中。

7.2.7 CACE 设施、信息架构和人员组织

每个 CACE 应用实例化对于其服务的 NASA 中心、工程或项目都是独有的。虽然实际的实现不同，但其基本特征是一样的。每个实现都关注于使工程师、设计者、团队领导和客户/利益相关者在并行活动和交流中具备更高的生产效率。本小节聚焦于该环境的三个方面：工作平台、支撑信息基础结构和设施保障人员职责。

7.2.7.1 工作平台

在共同工作的不同学科专家间同时进行交流，会产生或多或少的混乱。尽管团队领导的职责是维护工作环境的有序性，但工作平台本身必须设计成在参与者寻求增加交流和协作时，允许其维护任务的有序和延续。为了有效地实现这一目标，需要加大对基础结构资源的投入。

需要足够空间的房间来容纳学科交流讨论所需要的主动参与者、客户/利益相关者代表和观察员。CACE 负责人鼓励观察员向潜在的未来 CACE 用户介绍 CACE 使用的价值。

同样重要的是,注意房间经常会被重新布置。流程和需求改变时,CACE 平台必须随之改变。工作平台在旁观者看来可能是一个不断进步的工作空间。工作台、座椅、计算机工作站、网络连接、电源和可视化系统不断进行升级、修改或淘汰评估。

CACE 在可视化领域内的需求是独特的。当某个主题的专家需要与某个其他领域的专家小组或与整个系统的专家进行交流时,投影系统要能够切换到不同的工程技术工作站。当多个学科主题专家需要和不同的专家小组进行交流时,需要多个能够切换的投影系统。这通常需要 3~6 个投影系统,具备从指定的工作站切换到指定的投影系统的能力。此外,能够在工程技术工作站间切换的多投影系统需要匹配设置,这样就能在不影响室内其他活动情况下显示内容;或在此环节中,根据需要可以使整个小组重新聚焦。重构的灵活性是衡量 CACE 环境效率的指标之一。

7.2.7.2 信息基础结构

一个 CACE 系统不仅仅需要在设施上的大量投入,还极大地依赖信息基础结构。信息基础结构需求可以分解为三部分:硬件、软件和网络架构。

用于 CACE 平台的信息基础结构中硬件部分是系统中变化最快的部分。计算资源、通信结构、服务器、存储介质、可视化能力都从技术的迅速进步中受益。一个 CACE 平台必须能够利用这些技术进步在经济上带来的好处,必须有足够的灵活性利用新能力带来的好处。

CACE 信息基础结构中的主要成本来自软件。当前工程技术流程使用的许多软件属于建模和仿真方面,通常由商业软件商提供。支持工程数据交换、管理研究成果,支持跟踪、实施、管理平台活动的基础结构软件是 CACE 在整体上成功的关键。CACE 负责人的作用之一是决定软件开销如何支配,以及什么软件需要参与者和客户负责开发。

CACE 平台的网络架构是关键。信息在工作站、文件服务器和可视化系统间的实时流动需要重要的网络架构支持。此外,网络架构支持与外部顾问、外部学科专家,以及 NASA 中心内部之间的协同。网络架构的有效使用要求在网络安全和网络协同之间寻求平衡,这样可能需要修改、升级和重新配置。在地理上分布的 CACE 工作之间的协作是其自然延伸;因此,CACE 设施要有相应的工具、流程和通信能力支持这样的分布式研究。

7.2.7.3 设施保障人员职责

CACE 环境的运行维护需要一个核心职员团队,其职责覆盖全过程的 CACE 运行,以及 CACE 信息基础结构的操作和管理。

CACE 信息基础设施的操作和管理包括计算机工作站的配置、网络系统管理、文档开发、用户帮助服务,以及维护基础结构数据库、工具和 Web 站点的软件支持。

7.2.8 CACE 产品

CACE 产品适用于项目寿命周期各个阶段,并可以清晰地映射到与系统活动相关的各种输出;这些活动包括需求定义、权衡研究、决策分析和风险管理等。典型设计的 CACE 产品包括已辨识原始需求的需求概要;系统和分系统分析;功能结构和数据流;质量/能量/数据积累;使命任务设计和运行使用构想;工程技术权衡和相关结果;技术成熟度;问题、关注和风险;费用参量和/或底层费用估算;支持潜在未来工作的工程分析、模型和可用工具,以及未来分析建议表。

CACE 产品形式和内容在 CACE 环境和过程中变化多样。特定的 CACE 环境，所支持活动的目的/目标，活动是否被多个 CACE 团队支持，客户的最终使用及进度要求都作为某个方面体现在最终产品的内容和形式上。CACE 产品的识别、开发，以及最终打包交付的主要目的是在 CACE 活动后更加容易使用。

产品包括在研结果汇报，PowerPoint 幻灯片，正式报告和支持计算机辅助设计的模型，以及工程分析。不管什么形式，典型的 CACE 的最终产品总结了预定需求、研究目标期望和最终研究结果。

CACE 环境的灵活性使之能够支持的活动不局限于传统的工程设计研究（如独立技术评审、费用确认、风险和技术评估、路线图制定和需求评审）。此类活动的产品内容可能包括可行性评估、技术建议、风险辨识、成本核算、技术引入影响和实施途径，以及体系结构选择。

作为 CACE 产品正式交付给客户团队的补充，最终的结果和规划数据要存档到 CACE 环境中，以备将来参考和作为 CACE 内部交叉研究分析的案例。

7.2.9 CACE 最佳实践

本小节阐述 CACE 成功设计活动的最佳实践案例，其中三个主题（人员、流程和工具、设施）不论对于同处一地还是地理上分布的活动都适用。多 CACE 协同活动的很多经验都来自于 NASA 探索性设计团队的努力，即在 2005 财年进行的 OneNASA 多中心分布式协同设计活动。

7.2.9.1 人员

- **培训：**在 CACE 环境中工作的人员从特殊培训中获益。这个培训旨在让人员掌握有效协同工作必备的技能。培训的内容包括使人员适应 CACE 环境和流程所需要的相关技术。
- **特征：**在协同环境中的工作技能包括具有与众多陌生人一起工作的适应性，以及承担风险的愿望。需要具备能够思考并迅速反应的能力，作为团队成员开展工作的能力，直接与客户代表交流以确定需求的能力，以及正确做出设计决策的能力。提供技术保障的工程师还需要有能力快速而准确形成最终设计文档，并以专业方式展示设计。此外，CACE 团队领导还要具备额外品质，以便在协同设计环境中很好地发挥作用。这些品质包括组织和人员管理能力、系统工程技能和背景，以及广泛的一般工程知识。

7.2.9.2 流程和工具

- **客户参与：**管理客户期望是获得正面研究成果的第一要素。让客户逐渐明白 CACE 环境的应用范围和限制条件，以及请客户主动参与到协同环境中是非常重要的。
- **适应性：**CACE 环境必须适应依赖于研究类型和目标的流程，类型和目标在研究开始前通过商谈确定。适应流程的另一方面是必须在每项研究中安排具有相应工程和协同环境技能的工程师。
- **人员组织：**使用现成的团队好处是成员长期共同工作互相了解，并且熟悉工具和流程。缺点是固定团队没有新鲜感，难以紧随本专业领域最新的技术趋势和工具的发

展。保持一个全时的固定团队开销昂贵，经常是不可能。一个可行的方案是，一个全时（或接近全时）的领导团队附加一个工程技术团队。工程技术团队由工程师组成，成员可以轮换，或者适当长期留在团队中。另一个可选方案是在工程技术团队中安排部分来自客户团队的成员。

- **工具和数据交换：**一般来说，每个工程师应该使用其最熟悉的工程技术工具以使流程的效率效果最佳。CACE 环境应提供信息基础结构以集成由此产生的工程技术参数。
- **决策过程：**掌握决策和设计原理对于 CACE 客户来说有极大吸引力和极大价值，同时也是快速工程环境中面临的主要挑战。随着项目的进展，这样做的好处越发明显，并使 CACE 产品对客户更有价值。更长远地对于使命任务或设备的寿命周期、决策和设计原理的掌握比初期进行单点设计更有用。
- **交流：**CACE 环境促进团队成员间进行快速交流。快速变化的环境和并行工程活动使保持设计元素的“同步”成为一种挑战。这个挑战可以因有主动精神的系统工程师、经常性的更新、再加上系统工程支持及使用适当的信息基础设施得到解决。
- **CACE 环境标准：**在 NASA 的 CACE 环境内建立工具和技术的最低要求和标准集将促进多中心的协同。
- **计划：**做适当的计划和准备对开展有效的 CACE 研究很关键。客户若想放弃必要的预研活动或计划准备，必须认知和接受不良结果或低于期望的结果带来的风险。

7.2.9.3 设施

- **通信技术：**通信基础架构是协同 CACE 环境的中枢。应该使用能够有效访问 CACE 设施外部资源的技术。例如，具有即插即用能力的笔记本电脑。团队需要多部电话，手机接入是必要的。
- **分布团队连通性：**由于防火墙和其他网络问题的存在，地理上分布的团队之间快速联络和多个中心的活动所需信息的实时传输可能很复杂。在研究展开之前，应该对连通性和信息传输方法进行评审和测试。

7.3 选择工程设计工具

NASA 使用最前沿的设计工具和技术，来创造先进的分析、设计、概念开发手段，用于研发独有的航天产品、空间飞行器和科学实验产品。NASA 设计工作的多重属性需要使用广谱健壮的电子工具，例如，计算机辅助设计工具和计算机辅助系统工程工具。由于 NASA 项目的分布性和多属性，使用单一工具来开发所有产品是不现实的。然而，推进设计策略、流程和工具的标准化始终是 NASA 提升各层面能力的重点。

本节内容用于帮助在设计和开发航天产品、空间系统时，以及工具选择影响多个中心时选择适当的工具。

7.3.1 工程和项目考虑的事项

当选择工具来支持一个项目或工程的时候，必须在工作的早期确定顶层的约束和需求。

来自项目的对工具选择有影响的相关信息包括紧迫程度、进度安排、资源限制、无法避免的情况和约束。不满足项目主进度或费用太高而不能购置足够数量的工具，将不会满足项目负责人的需求。例如，一个工具如果因不能满足项目主进度需要大量的改动和人员培训，技术团队就不应该选择该工具。如果是对进行中的项目进行升级，现有的工具和经过训练人员的可用性是需要考虑的因素。

7.3.2 政策和流程

选择工具时，必须考虑包括中心、工程和项目、与其他中心协作的工程和项目在所有层次上的可行政策和流程。在下述讨论中，术语“组织”用于指代任何在 NASA 产品的设计或开发过程中为使用工具制定政策和/或流程的控制实体。换句话说，“组织”可以指用户的中心、其他合作中心、一个项目、一项工程、合作工程技术团体或者这些实体的任何组合。

政策和流程影响工具很多方面的功能。首要的是，有的政策规定组织内部如何正式或非正式控制设计。这些政策强调必须遵循的技术状态管理流程，以及被正式控制的数据对象类型（如图纸和模型）。很明显，这会影响到所使用工具的类型，以及这些工具的设计如何说明和控制。

组织的信息技术政策同样需要考虑，数据安全和输出控制（如武器交易国际规章）是要考虑的两个重要的信息技术政策，它们会影响特定设计工具的选择。

组织的政策也规定设计数据（由工具产生）格式方面的需求。对于各协作方共享的信息可能需要特定的格式。其他需要考虑的是组织的质量管理流程，控制软件工具的版本，以及它们的确认和验证。还有一些关于对保障关键飞行工程和项目工具使用者培训和资格认定的政策。这在选择一个新工具而导致需从原有的工具过渡到新工具时尤为重要。因此，工具供应商提供的培训质量保证是选择工具时需要考虑的重要因素。

同样，如果采购支持多中心协同工作的工具，那么工程政策可能会规定所有参与的中心必须使用什么工具。如果各个中心有自由选择自用工具支持多中心工程和项目的权利，那么每个中心的政策就要考虑保证各个中心间兼容性的问题。

7.3.3 协同

由于必须要有各个复杂的专门学科交互合作才能完成总体设计，设计流程是高度协同的。工具是成功协作的重要组成部分。为了在这个环境中顺利选择和集成工具，需要对用户的组织规模、需求的功能、共享数据的性质、对工具应用的理解等方面信息有清晰的理解。这些因素将确定许可证的数量、主机容量、工具能力、信息技术安全需求和培训需求。在一个大范围群体内共享公共模型，需要以某种控制手段推进设计的机制。数据管理工具的有效使用能够帮助控制以统一命名规则、标记和设计技巧构成的协同设计，确保分布式设计工具的兼容性。

7.3.4 设计标准

对于不同的领域或学科，都有必须遵守的行业或中心制定的标准，特别是在设计硬件时。

这在设计机械部件时将最为明显，用于对部件建模的计算机辅助机械设计软件包必须能够满足特定的标准，例如，模型精确度、装配尺寸和公差、构造不同几何外形的能力，以及添加注解以描述如何建造和检查该部件的能力。当然，对所有类型的产品都必须考虑这些问题。

7.3.5 现有的信息体系结构

在决定使用任何新工具时，应该对 NASA 总局和中心的相关信息体系结构进行评估，评估重心在于新工具与现有工具的兼容性和重复程度上。典型的体系结构包括数据管理工具、中间件或综合基础设施、网络传送容量、设计分析工具、制造设备、经核准的主机和客户环境。

最初的重点一般放在当前的需求，而工具的可测量性、信息基础设施支持也应该被考虑。可测量性指标可以使用客户数量，或使用成功支持每个用户不间断使用系统的容量。

7.3.6 工具接口

信息接口普遍存在，在任何交换信息的时候都要使用。

这是协同环境特有的性质。在此会产生效率降低、信息丢失，以及错误发生等问题。与其他分析工具进行交互可能需要一种有组织的需求。理解自身团队和其他设计团队使用哪一个工具进行交互，以及自身团队的输出如何驱动下游的设计能力，对于保证数据的兼容性至关重要。

对于计算机辅助系统工程工具，鼓励用户选择使用与国际对象管理组织（OMG）的系统建模语言 SysML 标准兼容的工具。SysML 是统一建模语言 UML 为系统工程开发的专用版本。

7.3.7 互操作性和数据格式

互操作性是选择工具时需要考虑的重要因素。工具必须使用能够被数据最终用户能够接受的格式来描述系统设计。任何被选用的工具都要包括相关的数据交换格式和工业标准数据格式。随着 NASA 承担的多中心工程和项目日益增多，对不同工具间及相同工具不同版本间的互操作需求越来越关键。真正的互操作性能减少人为失误，降低集成工作的复杂度，从而可以降低费用开支，提高生产效率和产品质量。

当考虑所有最终用户的需求时，实现互操作性明显地变得较为困难。以下是三种各有优缺点的主要实现途径：

- 让所有员工熟悉大量系统工具及其与最终用户相关的用途，如此可形成广泛的能力，这可能无法负担和不太可行。
- 要求任何所使用的工具之间都能进行互操作。例如，每个工具都要能够以某种可以被所有其他工具轻松和正确转换的数据类型传送模型数据。需要考虑近年模型数据交换标准取得的进展。虽然这对于很多用户都是一个理想的解决方案，但能涵盖所有最终用户所需信息的标准数据格式尚不存在。
- 规定组织内的所有成员使用相同工具的同一个版本。

7.3.8 向后兼容性

在持续若干年的工程和项目中，经常需要处理 3~5 年前的设计数据。然而，访问这些

陈旧的设计数据可能极端困难和昂贵，或者由于工具提供商终止服务及不再提供旧版本的工具而无法读取数据。维护访问数据能力的策略有，与工具供应商签订更长服务的特别合同、用中间格式存储设计数据、不断将旧数据转化到新的格式或者按照需要重新产生新格式下的数据。工程组织应该在仔细考虑费用和风险后选择最为合适的策略。

7.3.9 平台

许多软件需要在不同的硬件平台上运行，而一些软件仅能在特定环境下良好运行或仅支持特定的操作系统版本。在开源情况下，操作系统的许多变化可能不完全支持所需的工具。如果认为工具需要一个新平台，就需要考虑由此而带来的额外采购费用和管理服务费用。

7.3.10 工具技术状态控制

工具技术状态控制就是在采用新版本工具的新功能和整个工具链组件平稳运行之间进行权衡。这在（多个供应商提供的）工具组件异构时尤为困难。对一年一次或一年两次的模块升级策略需要进行有效的管理。此外，用户自定的工具升级时间导致的平台差异性，也要求提供更多的支持。

7.3.11 保密性/访问控制

特别需要考虑所有设计数据的敏感性和访问需求。联邦政府和 NASA 政策要求对所有工具进行评估，确保对数据的安全保密控制，以维护数据的完整性。

7.3.12 培训

对于经验丰富的设计师来说，许多工具都有相似性。但是，每个工具都使用不同技术来实现设计功能，每个工具都包含一些独特的工具集，需要对使用人员进行培训。许多工具供应商会提供跟踪指导和集中培训，分发培训材料和应用案例。培训的时间和费用及使设计人员精通工具的时间花费都很可观，在决定使用新工具时需要认真考虑这些因素。

培训的负面影响是采用新工具时需考虑的重要因素。在启动使用新工具前，决策组织应考虑主要工程和产品交付的进度安排。合同规定的时间是否够用？建议组织实施逐步采用新工具的策略，在设计人员学习新工具并渐渐熟悉新工具的同时保留使用旧工具。当专家团队将所有实际工作转移到使用新系统时，在同一个团队内同时使用原有系统开展实际工作是个好的做法。新旧工具的某种重叠能够确保工具转换的适应性及工程和项目的不间断顺利进行。

7.3.13 许可证

许可证提供并控制对产品或产品系列中各种模块和组件的使用权。选择工具包时要相应考虑许可证问题。许可证可以是物理的，如插入串行或并行端口的硬件钥匙，也可以是需要或不需基础管理结构的软件。软件许可证可以是流动的（基于先到先服务规则被多台计算

机共享),也可以是锁定的(指定计算机使用)。一个好的许可证策略必须在选择工具之初就确定。这个策略要考虑到工程和项目需求、约束,以及其他如培训和使用等相关因素。

7.3.14 供应商和用户保障的稳定性

在选择任何保障设备或者工具时,供应商的稳定性极其重要。如果对工具(直接地)或对基础设施(间接地)进行巨额投资,全面考察供应商公司的稳定性以确保其能够持续提供工具保障是非常重要的。产品的成熟度、稳定的用户基础、培训能力和财政状况都反映出供应商在产品市场中的生存能力。此外,一个负责任的供应商应为客户提供多种形式的保障。其中之一是为用户提供基于 Web 的用户可访问的知识库,汇集已经解决的问题、产品文档、用户手册、白皮书和指导书。电话热线服务对于自身无保障机制的客户非常有价值。问题的解决或加剧过程与用户直接参与跟踪和优先解决关键问题有关。销售人员、应用工程师和售后服务工程师一起现场解疑可以明显缩短发现和解决问题和确定相关需求的时间。

7.4 人因工程

人因工程学致力于对人机界面和人类组织的研究、分析、设计和评估,重点在于人类影响系统运行的能力和限制。人因工程的问题涉及各种(正常、偶发、紧急)运行条件下系统寿命周期中的各个方面,包括设计、建造、测试、运行和维护等。

在复杂的航空航天系统中,人是关键的组成部分,包括设计人员、制造人员、操作人员、地面保障人员和维护人员。系统的所有单元都受人的行为影响。在人机系统中,有四个途径可以提升系统性能、减少错误、提高系统容错能力:(1)人员挑选;(2)系统、接口和任务设计;(3)培训;(4)技术规程改进。提升系统性能的有效措施都与这四个方面有关。首先,根据从事的工作和置身的环境严格挑选人员。其次,设备和系统可以设计成容易使用、方便学习并且有容错能力。再次,可以对人员培训使他们熟悉所要完成的任务。最后,改进任务或流程也很重要。

人因工程关注于系统中人机接口部分。考虑所有与系统交互的人员,而不仅是操作人员;处理组织系统及硬件;检查所有交互类型,而不仅是硬件和软件接口。人因工程专家的任务在于考虑人类组件,确保硬件、软件、任务和环境的设计与参与系统交互的人的感觉、知觉、认识和身体特征等相协调。人因工程专家需要阐明为什么在系统的分析、设计决策中应当考虑与人有关的问题或特征,检验和解释设计方案如何影响人在全系统性能和费用上的作用。随着系统复杂性的增加,需求间发生冲突的可能性也会增加。完善的人机界面也会在生成如既能方便初学者学习使用又能使专家有效使用的系统方面出现冲突。人因工程专家要识别这些冲突的权衡因素和约束,并为平衡这些冲突提供指导。人因工程的应用遍及需要考虑人和组织的性能、错误、安全性和舒适性的领域。目标是引导和促进设计。

有别于其他学科专家,人因工程专家具备特有的知识结构、工作方法、工作范围和工作目标。人因工程专家具有人类行为方面的一般和专门的专业知识。有许多关系到应用人类行为知识的学科,包括心理学、认知科学、认知心理学、社会学、经济学、教育学、生理学、工业心理学、组织行为学、通信学和工业工程学。项目负责人和流程负责人应该向工程技术主管或安全性与使命任务担保主管咨询,以获得寻求适合其特定活动的人因工程专家方面的建议。

在整个系统工程技术流程中，都应该为技术团队配备人因工程专家，他们能够建立适合特定流程和项目的人因工程分析技术和试验。人因工程专家不仅在产品开发过程中帮助解决问题，还能确保验证试验和完整性技术精确符合人的使用习惯。早期参与到流程中特别重要。在系统设计的早期就加入人因工程，可以确保人机需求是设计出来的而不是后来更正的。有时，后期分析的结果可能导致对前期的分析进行复查。例如，由于技术突破，设计和规划中无法预见的技术困难，或是任务分析表明某些情况下某些分配给人的任务超出了人自身的能力等情况，功能分配通常都会随设计的进行不断调整。

在需求定义阶段，人因工程专家确保与人因工程相关的目标和约束包含在系统的整个计划中。人因工程专家必须确定与人因工程相关的问题、设计风险，以及关系到每个人机组件的权衡因素，并将其作为项目需求的一部分归档，使其在设计阶段予以适当考虑。从人因工程角度来看利益相关者期望定义，利益相关者不仅包含那些指定建造系统任务的人，还包括那些在系统投入运行时使用该系统的人。这种方式服从自顶向下（系统将要完成什么功能）和自底向上（怎样预期系统能达到的功能）的需求产生过程。人因工程专家对运行使用构想的贡献很关键。对系统中人的作用和对人所承担任务类型的期望，是所有系统硬件和软件需求的基础。被动乘客和主动操作者之间的区别影响重要的设计决策。乘员的数量影响关于生活和储存空间，以及乘员进行操作和维修可用时间的后续决策。人因工程专家确保恰当的系统设计能定义系统未来运行时的环境范围和任何影响人类组件的因素。这些因素中许多需要适应人和机器的忍耐程度。需求中可能需要明确可接受的大气条件，如大气温度、大气压力、大气成分和大气湿度等。需求中也可能需要确定噪声、振动、加速度、重力的可接受范围，以及防护服的使用。需求中可能还包括需要承受在正常操作范围之外出现的有害或紧急情况。

7.4.1 基础人因模型

进行人和组织的分析、设计和试验，很重要的一点是要有一个清晰的问题相关范围的框架。下列模型定义了评估人的作用影响的边界和组成。

人因交互模型（见图 7.4-1）提供了一些在规划、分析、设计、试验、运行和维护系统时需要考虑的参考内容。详细的参考内容清单应当根据特定的待开发系统来生成并客户化。这里提出的模型是根据 David Meister 的《人因学：理论和实践》一书建立的，描述了人和系统如何进行交互，并加入了交互中的环境影响。这个模型阐明了系统中的人和机器组件间的信息流动过程。

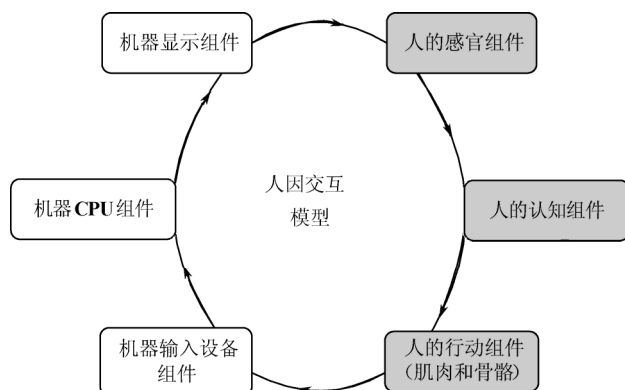


图 7.4-1 人因交互模型

图 7.4-2 列出了在系统计划、分析、设计、试验、运行和维护时需要考虑的人因流程阶段参考点。

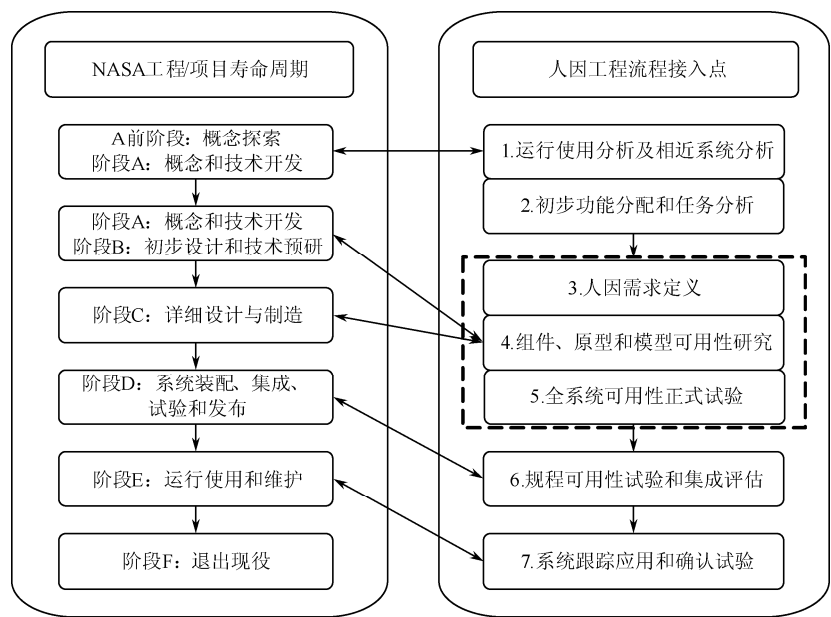


图 7.4-2 人因工程流程及与 NASA 工程/项目寿命周期的联系

7.4.2 人因分析和评估技术

表 7.4-1 提供了一些关于人和组织分析评估的相关技术，有助于在应用时确保考虑到相关的人和组织因素。这些人因分析方法用于系统分析，提供关于人的能力的数据，预测人机系统的性能，以及评估人机系统性能是否满足设计标准。许多方法中都包含判断，因此强烈依赖于分析人员的专业知识和分析能力。此外，无论有经验的还是没有经验的操作人员，都可以提供关于原有系统优缺点，以及新系统应如何使用的有用信息。

这些方法适用于系统设计的所有阶段，并随着系统开发的进展而更加特殊和详细。尽管人因工程原理在一般的层次上研究和理解，但应用时需对其进行裁减以适应具体设计阶段。每类分析需要不同类型信息，所以这些方法之间不能相互替换。分析的输出或产品写入规范文档中（如操作需求文档、运行使用构想、系统需求文档等），并进行正式的评审（如运行使用需求评审、系统需求评审、系统定义评审、初步设计评审、关键设计评审、生产准备状态评审和工程实施评审）。

表 7.4-1 列出的条目并不是完整的，主要是举例说明用于评估系统设计和开发的通用方法的范围和适用性。

表 7.4-1 人和组织分析技术

流 程	人类/个体分析	附加的组织分析
A 运行使用分析		
定义	当应用于人因工程时，此即对工程化操作进行分析	
目标	获取操作人员或者维护人员使用新系统时可能遇到的情况或事件的相关信息。通常系统工程师或运行分析师完成运行分析。人因工程专家应该也是分析小组成员，以掌握操作人员或维护人员的重要活动	

续表

流 程	人类/个体分析	附加的组织分析
输入	申请指南、计划文档、系统需求文档和专家建议	
流程	咨询系统工程师和系统用户,为系统操作人员和维护人员提炼有用的信息	评估个人和组织之间的信息流与物流。评估在不同类型的组织、结构、分布状态下的系统运行
输出	包括(正常运行、硬件和软件故障、紧急事件)后果的详细想定;对操作人员和维护人员面临事件的文字描述;预测的运行(列出可行的运行,以及可能超出系统承受力的运行);假设;可能影响系统性能的约束;环境;系统运行维护需求列表	新的或经过调整的工作流,以适当补偿组织影响
B 相似系统分析		
定义	当应用于人因工程时,此项检查原有系统或运行中系统,得到对新系统有用的信息	
目标	得到对计划中的新系统有用的最佳实践经验和教训。来自于运行中系统的经验,是需要特别注意的有价值信息	
输入	结构化的观察、面谈、提问、活动分析、事故/事件报告、维护记录 and 培训记录	
流程	获得关于可操作性、可维护性、系统使用所需配备人员数量的数据。明确系统运行和维护需要的技能,以及使操作人员熟练掌握技能所需的培训。获取关于前期人因工程设计时遇到的问题,以及已有或使用中系统用户所遇到的问题	确定现有系统的组织层次结构和管理方式(集中式还是分散式)
输出	可能影响人员的环境因素标识;对工作负荷和工作压力的初步评估;对于选择、训练和设计所需的技能及其影响的评估;未来的职员和人力需求估算;操作人员和维护人员需避免的问题标识;系统功能重新分配带来的需求和后果评估	评估技术状态对性能的影响和潜在风险
C 关键意外事件研究		
定义	当应用于人因工程时,此项为操作人员和维护人员确定难题来源,或确定操作系统(或其仿真系统)中的难题来源	
目标	分析和设定系统中错误和难题的根源,当系统已经运行并发现或怀疑发现难题,但是这些难题的性质和严重性尚不清楚时,这点尤为重要	
输入	操作人员和维护人员记录的意外事故、接近发生的事故、出现的错误和接近出现的错误	
流程	与大量操作人员/维护人员面谈;对事件和事故进行分类;利用人因工程知识和经验估计难题的根源,以及将来的研究解决方案;重新设计以消除麻烦	追踪个人和组织之间的难题,映射相关的责任,进行处理安排
输出	在系统运行或维护中严重的人因难题的来源,相应难题的解决方案	映射过程产生的潜在差异和间断的标识
D 功能流分析		
定义	当应用于人因工程时,此为确定系统需求的结构化技术。分解系统必须执行的功能或活动序列	
目标	提供能够达到系统需求的功能序列,以及确保系统能够执行预定使命任务必须考虑的详细系统功能列表。这些功能用于解决权衡问题,并确定操作人员、设备、软件或其组合之间的功能分配。当系统需要(如面向软件的)二元决策时,决策活动分析经常用于代替功能流分析	
输入	运行使用分析、相似系统分析、活动分析	

续表

流 程	人类/个体分析	附加的组织分析
流程	顶层功能逐渐扩展到包含越来越多详细信息的低层。如果需要额外的关于如信息需求、信息源、潜在问题，以及诱发错误特征等因素的细节，还需要进行行动信息分析	将功能流映射到相关的组织结构
输出	功能流程图	整体映射引起的任何后勤保障或责任上的差异标识
E 行动信息分析		
定义	当应用于人因工程时，此项通过确认产生行动或决策所需的信息，详细阐述在功能流程图或决策-行动图中的每一个功能或行为。这种分析经常利用与每个功能和行动相关的数据源、潜在问题，以及诱发错误特征等信息	
目标	在将功能分配给各个机构前，提供更多的细节	
输入	来自相似系统分析、活动分析、关键事件研究、功能流程图和决策-行动分析的数据，以及来自有丰富知识专家的评议和数据	
流程	详细阐述功能流或是决策-行动分析中定义的每个功能或行动	将相关组件（功能、行动、决策）映射到相应的组织结构中
输出	操作人员与系统接口的信息需求详细列表，对所需人员储备的预先估计，保障需求，以及潜在问题和可能解决方案的列表。通常生成对硬件、软件或流程改进设计的建议	综合映射引起的任何物流和责任上的差异标识
F 功能分配		
定义	当应用于人因工程时，此项是给每个系统功能、行动和决策分配硬件、软件、操作人员、维护人员或是这些要素结合的技术规程	
目标	帮助确定用户所需的技能，初步估算人员、培训、程序需求并评估工作量。功能流和决策-行动分析不定义执行功能的人或机器	
输入	功能流分析，决策-行动分析，行动信息分析，相似系统的已有工程经验，机器和软件的使用性能现状，已知的人员能力和局限性	
流程	确定并区分出于安全、工程技术限制、人自身局限性或系统需求的原因而必须分配给个人或设备的功能。列举出剩余的功能，这些功能可能是需要人工执行，或者是需要人和设备的结合执行。准备对功能实施方案的描述。针对每种设计方案建立赋权准则。对比这些方案在根据给定准则执行给定功能时的有效性	初始功能分配完成以后，在相关组织规范、价值、组织接口对物流和管理的影响方面评估功能分配
输出	系统功能到硬件、软件、操作人员、维护人员或是这些要素结合的分配。对于分派给人员的功能进行的任务分析	对功能、管理或两者结合修改的潜在影响列表
G 任务分析		
定义	当应用于人因工程时，该项是产生人在系统中要完成任务的有序列表的方法	
目标	开发所有将要顺序进行的任务分析的输入。一个时间序列分析图能够提供任务间的时序关系——操作人员或维护人员的行动序列、每个行动所需的时间、每个行动发生的时刻	
输入	来自以上方法的数据，以及来自有类似系统开发经验的专家提供的补充信息	
流程	人因工程专家和项目主题专家列出并描述所有任务，利用补充信息将这些任务分解成子任务	对所有任务分组并分配给相应的组织，评估所需技能、交流和管理能力的范围。依据现有组织的标准运行程序、规范和价值体系评估新的需求

续表

流 程	人类/个体分析	附加的组织分析
输出	人员在系统中所要完成的所有任务的有序列表。关于信息需求、必须做出的评估和决策、任务时间、操作人员行动和环境条件的细节	确定分组层面的工作量、管理影响和培训需求
H 故障树分析 (FTA)		
定义	当应用于人因工程时, 该项确定可能使特定系统发生失效、故障和灾难的事件组合。故障树、失效模式和影响分析都是基于错误的分析	
目标	预测操作人员和维护人员可能的错误操作, 并尽力在设计上避免。人因分析的局限性在于每个事件只能定义在两个可能状态上, 对人类行为很难进行精确概率预测	
输入	以上描述的方法中所有的输出数据, 以及人员可靠性方面的数据	
流程	利用(逻辑门)符号构建故障树, 这些符号代表事件和后果, 可以描述事件之间的逻辑关系	预测个人和组织间工作流中可能发生的错误和断点, 包括标准的组织运行程序和可能的系统事件之间不可预测的交互
输出	各种非预期的工作流相关事件的发生概率, 导致这些事件的可能的工作序列, 能够降低意外发生概率的敏感因素的标识	组织的工作流接口带来的各种非预期事件的发生概率, 导致这些事件的可能的工作序列, 能够降低意外发生概率的敏感因素的标识
I 失效模式和影响分析		
定义	当应用于人因工程时, 该项是确定可能引发系统中错误事件因素的方法	
目标	推断一个或多个组件(含操作人员和维护人员)中的故障对系统性能的影响后果, 以及这些后果的发生概率	
输入	以上描述的方法中所有的输出数据, 以及人员可靠性方面的数据	
流程	分析者确定操作人员或维护人员在执行子任务或功能时可能产生的各种错误。估算每种错误发生的概率或频率。通过跟踪功能流程图直到其最终结果来推断每类错误所带来的后果	识别系统密切相关的可能的组织实体和行为(如政治实体和行为), 评估发生的概率和后果带来的影响
输出	对系统运行可能产生关键影响的人为故障列表, 由于人为错误所带来的系统或子系统失效的概率, 可以降低严重系统故障概率的需要改进或被替代的人员任务或行动标识	对系统运行产生关键影响的组织行为列表; 由于组织行为而带来的系统或子系统故障发生的概率; 可以降低严重系统故障概率的需要改进或被替代的组织价值、文化或标准操作流程
J 链路分析		
定义	当应用于人因工程时, 该项检查系统各组件间的关系, 包括仪表盘、控制面板、工作站和满足特定目标工作区域的物理布局	
目标	确定人机界面物理布局的效率和效能	
输入	来自活动、任务分析、对功能系统或仿真系统观测的数据	
流程	列举所有人员和设备。评估设备之间、操作人员之间和设备与操作人员之间的链接频率。评估每个链路的重要性。计算每个链路的频度价值。从最高价值的链路开始, 连续地加入较低链接价值的设备并调整使链接最小化。在分配空间中安排布局。根据最初目标评估新的布局	在个体和组织层面上评估链路
输出	面板、工作台或者工作区域的布局建议	在保证最佳的个人和组织性能前提下, 调整面板、工作站或工作区域布局

续表

流 程	人类/个体分析	附加的组织分析
K 仿 真		
定义	当应用于人因工程时, 本项是用于预测系统性能的基础工程技术或人因工程方法, 包括可用性试验和原型开发	
目标	当系统不存在或因为复杂、危险及昂贵而不允许用户在系统或系统组成部分上进行试验或培训时, 预测系统或系统组成部分的性能	
输入	硬件、软件、功能、任务分析中阐明的任务、操作流程	
流程	用户在适合部分或所有输入的模式或样机上运行典型的任务	在可能的组织模型中评估个体的性能
输出	系统性能预测、工作量评估、备选技术状态评估、操作流程及培训评估、确定引发事故和错误的状况, 以及人员和设备间的错误匹配的标志	在各种组织情况下评估系统性能、评估工作量、评估备选技术状态、评估操作流程及培训、确定引发事故和错误的状况, 以及人和设备间的错误匹配
L 受控实验		
定义	当应用于人因工程时, 本项是一个高度受控和结构化的对某些变量精细处理的仿真实验	
目标	回答一个或多个假设, 缩小用于仿真的备选方案数量	
输入	来自以上所有方法的数据	
流程	选择实验设计方法; 确定独立、非独立和受控变量; 安排实验、仪器、设备和任务; 准备实验协议和操作指南; 选择实验主题; 运行实验; 对实验结果进行统计分析	确定适当、可行的组织层次
输出	某些变量对另外一些变量的影响的定量化描述, 以及可选择的技术状态、流程或环境之间差别的定量化描述	某些组织变量对另外一些组织变量影响的定量化描述, 以及可选择的组织技术状态、流程或环境之间差别的定量化描述
M 运行序列分析		
定义	当应用于人因工程时, 本项是用于对系统进行仿真的强有力技术	
目标	能够对操作人员之间、操作人员与设备之间的关系进行可视化表现; 确定系统接口问题; 明确辨别可能无法实施的决策。在试图达到相同目的时, 费用低于相应的样机、原型或者计算机程序	
输入	来自以上所有方法的数据	
流程	用竖列表示时间、外部输入、操作人员、机器和外部输出。用特定符号体系绘制自顶向下随时间标度(行动、功能、决策)的事件流	在初始分析完成后, 根据相应的组织对结果进行分组
输出	系统各单元之间的功能关系、材料流或信息流, 物理的和时序的运行分布、子系统的输入和输出, 不同设计方案的结果, 以及可能遭遇困难的原因等基于时间的图表显示	所需技能、交流过程和管理能力的评估。在各种组织结构下的性能评价
N 工作量评估		
定义	当应用于人因工程时, 该项评价操作人员和职员的任务量, 或是个人在规定的时间内完成所分配任务的能力	
目标	确保操作人员的工作量保持在一个合理的层次上, 确保工作量在操作人员之间分配的公正性	
输入	从上述方法中获得的任务时间、频率和精度数据, 以及来自有经验专家的判断和估计	
流程	DOD-HDBK-763 推荐一种用于估计完成一项任务所需时间的方法, 任务根据可用时间和安排完成任务的时间划分。有三种方法: 性能指标、生理指标、活动中或活动后的个人主观工作量	在初始分析完成后, 根据相应的组织对结果进行分组

续表

流 程	人类/个体分析	附加的组织分析
输出	对在特定时间内特定任务的估算工作量的定量评估	所需技能、交流过程和管理能力的评估。 在各种组织结构下的性能评价
O 情势感知		
定义	当应用于人因工程时，该项评价操作人员和全体职员对任务和当前情势的感知能力	
目标	提高操作人员和维护人员对维护系统运转的安全性和效率的感知能力	
输入	所有以上所列分析的结果	
流程	建议采用不同的方法，包括情势感知分级技术、情势感知行为实绩分级度量、情势感知全局评估技术、情势感知验证和分析工具	搜集组织决策结构和流程，构造组织情势感知剖面映射
输出	对特定时间内特定任务的情势感知能力的量化估计	可能的差异、间断和不足的标识
P 性能建模		
定义	当应用于人因工程时，该项是预测基于当前认知研究的人员行为的计算过程	
目标	在建立原型前，预测人的能力和受限之处	
输入	所有以上所列分析的结果	
流程	输入来自于以上的分析的结果。输入当前相关环境和机器参数。用快速仿真交叉扫描数据，得到错误类型出现的频率	适合相关组织行为的尺度
输出	操作人员之间、操作人员和设备之间的相互关系，接口问题和无法实施的决策标识	个人与组织之间的相互关系。组织接口问题和无法实施的决策标识

7.5 环境、核安全、行星保护和资产保护政策约束

7.5.1 美国国家环境政策法令和行政法令

7.5.1.1 美国国家环境政策法令

美国国家环境政策法令（NEPA）是国家（美国）保护人类环境的基本法案。NEPA 设定了增强和保护环境的国家目标。NEPA 还提供保证所有联邦机构能够服从的流程需求。服从 NEPA 标准是项目或使命任务实施的一项关键内容。NEPA 要求所有联邦机构在采取任何行动之前要充分考虑所规划行动和活动的环境价值，考察这些行动和活动是否会对人类共同生活的环境产生明显的影响。NEPA 指导各机构对规划的活动考虑可选择的方案。基本上，NEPA 需要 NASA 决策者把 NEPA 流程集成到系统早期计划中，确保适当考虑到环境因素，就像考虑技术因素和经济因素那样。NEPA 也是一个环保法规，它要求适当处理可用信息并及时提供给 NASA 决策者，使其在最终采取行动之前考虑计划行动和活动在环境方面的后果和影响。环保方面信息应该向公众公开，以及向其他的联邦、州和地方机构公开。NEPA 并不要求所有计划的行动和活动都对环境没有任何影响，或是采用对环境最有利的方案，或是做出有利于环境最明智的决策。NEPA 要求决策者将环境影响作为一个因素在进行行动决策时予以考虑。

NASA 活动通过各种特定负责单位组织实施,如 NASA 总部、NASA 中心(包括下属设施,如沃洛普斯飞行靶场^①、白沙试验靶场^②、米丘德总装工厂^③)、使命任务主管、工程办公室或使命任务保障办公室。这些单位的领导和负责官员,对确保在其单位采取行动和进行活动之前将 NEPA 流程集成到组织内项目计划活动中负有主要责任。负责单位对确保活动过程符合存档的管理需求负有责任。NEPA 职责并非由领导和负责官员直接完成,通常 NASA 的每个中心都有一个环境管理办公室,代表中心负责 NEPA 活动的执行。环境管理办公室执行 NEPA 活动中的主要职责和工作层面的职责,如评价规划的活动,开发、评审和批准所需要的文档,对项目负责人提出建议,签署工程和项目中对环境没有影响或影响很小的环境决策文档。当然,遵从 NEPA 准则并按时完成 NEPA 活动的最终责任者是工程和项目负责人。既然环境管理办公室作为负责单位的基本功能支持部门,并委派了实施执行责任者,因而术语“负责单位”同时包括 NASA 设施中贯彻实施 NEPA 的组织。如果负责单位需要被进一步定义,将会详细说明。如果活动由 NASA 中心或其下属设施提出,或由使用 NASA 中心或其下属设施服务的单位提出,则负责单位为该 NASA 中心;如果对下属设施进行了授权委派,负责单位为其下属设施。

在 NASA 项目规划中发现在实施合理方案的能力方面遇到明显阻碍之前(即在制定实施项目相关决策之前),必须完成符合 NEPA 的文档。当允许考虑广泛的可选择方案时,应该把环境规划因素集成到 A 前阶段的概念探索阶段中。在阶段 A(概念研究与技术开发阶段),制定的决策可能会影响到阶段 B(初步设计阶段)。至少,在阶段 A 的概念开发阶段,应当启动对环境的评价。在这个阶段,项目负责人有最大限度的权利调整计划以减轻或者避免重要的环境敏感因素,以及平衡规划 NEPA 流程以避免在随后的项目进程中在进度和费用方面出现令人不愉快的意外。在完成 NEPA 流程前,没有哪个 NASA 官员能够采取影响环境的行动或限制合理方案选择的行动。

在项目计划初期就确定环境方面的需求,最终会有助于节省预算和加快进度。关于 NASA 工程和项目符合 NEPA 要求的进一步细节可以查阅 NRP8580.1《国家环境政策法案(NEPA)》和第 12114 号美国行政法令。

7.5.1.2 联邦在国外主要活动的环境影响

第 12114 号美国行政法令(EO 12114)是“为建立联邦机构内部技术规程来处理他们在美国之外的活动对环境产生的显著影响”的目的而发布的。该项行政法令还特别提到其目的是使联邦机构决策者能够得到潜在的环境问题的提醒,并将这些问题作为他们决策时考虑的因素。此外,这些决策者还必须时刻考虑到外交政策、国家安全和其他相关环境因素。

NASA 的法律总顾问办公室或者其代理人是任何涉及 EO 12114 问题事项的 NASA 联络机构和官方代表。因而任何与 EO 12114 相关的活动或对 EO 12114 的法律解释,都需要向法律总顾问办公室的代理人咨询并得到他们的同意。活动负责单位和本单位环境管理办公室要对可能影响全球环境或者影响美国领土之外环境的活动严密关注,并通报给 NASA 总部环境管理部门。相应的,NASA 总部环境管理部门要协同法律总顾问办公室、对外联络主管助理和其他 NASA 相关组织,协助活动负责单位制定合适的行动计划(如经过法律总顾问办公室同意的计划)。NASA 工程/项目遵从 EO 12114 要求的详细信息见 NPR8580.1。

① 沃洛普斯飞行靶场(Wallops Flight Facility)位于美国弗吉尼亚州东海岸,建于 1945 年,由戈达德航天飞行中心负责管理。

② 白沙试验靶场(White Sands Test Facility)位于美国新墨西哥州,建于 1963 年,由林登·约翰逊航天中心负责管理。

③ 米丘德总装工厂(Michoud Assembly Facility)位于美国路易斯安那州新奥尔良,是马歇尔航天中心的一部分。

7.5.2 关于放射性物质的环境影响

NASA 对在正常和非正常条件下运载火箭和空间飞行器携带放射性物质进入太空有程序上的要求，需要对潜在的风险进行特征分析并形成报告。根据计划使用的放射性物质数量和对公众和环境潜在威胁，核发射安全审批要求采取不同的评审和分析程序和审批等级。关于这些需求的详细内容参见 NPR 8715.3 《NASA 通用安全工程需求》。

对于任何采用放射性同位素能源系统、放射性同位素加热单元、核反应堆或主要采用核资源的空间使命任务，必须依照 1996 年 5 月 8 日修订的第 25 号总统令/国家安全委员会备忘录“可能带来大规模负面环境影响的科学技术实验和发射核系统进入太空的活动”中的第 9 条，获得总统办公室的批准。审批决策的基础是已经核定的评审程序，包括由来自 NASA、能源部、国防部、环境保护署的代表，以及来自原子能管理委员会的技术顾问组成的跨机构核安全特别评审小组（INSRP）进行独立评估。这个评审程序首先开发一个飞行器发射数据手册（即描述使命任务、发射系统、包含环境和发生可能性的潜在事故想定等信息的纲要）。能源部根据这份数据手册给出空间使命任务初步安全分析报告。通常需要形成三份安全分析报告——初步安全分析报告、修正的安全分析报告（最终安全分析报告的草案）和最终安全分析报告，并提交给使命任务的跨机构核安全特别评审小组。这些文档由负责提供核动力系统的能源部项目办公室开发。

跨机构核安全特别评审小组负责核安全/风险评估，并将评估结果写入安全性评价报告。安全性评价报告包含一个对使命任务放射性风险的独立评估。能源部将安全性评价报告作为接受安全分析报告的基础。如果能源部部长正式接受安全分析报告-安全性评价报告组合文件，则 NASA 管理机构使用该组合文件进入正式审批程序。

NASA 将安全分析报告、安全性评价报告分别提供给跨机构核安全特别评审小组中其他的政府机构人员，请求他们对这些文档进行评估。在获得这些机构的反馈后，NASA 对安全分析报告、安全性评价报告和其他与发射相关的核安全信息进行内部管理评审。如果 NASA 管理机构建议执行发射，则需要向总统办公室的科学技术政策办公室负责人发出核安全发射许可的请求。

NASA 总部负责 NASA 使命任务中该程序的实施。传统上这项活动需要获得喷气推进实验室（JPL）^①的帮助。能源部通过分析冗余的动力系统硬件对数据手册中定义的不同事故想定的反应，以及评估该使命任务对公众和环境构成威胁的潜在放射性后果及风险，为该程序提供支持。肯尼迪航天中心负责监督数据手册的开发，传统上与喷气推进实验室共同描述事故环境并形成数据手册。作为分包商，肯尼迪航天中心和喷气推进实验室需要提供支持数据手册开发的相关信息。为使命任务最终选定的开发团队负责提供有效载荷描述，说明核动力系统如何集成到宇宙飞船上，说明使命任务需求，并为肯尼迪航天中心和喷气推进实验室开发数据手册提供支持。

负责控制和处理发射到太空中放射性物质的使命任务主管助理、NASA 中心负责人和工

^① 喷气推进实验室（Jett Propulsion Laboratory）位于美国加利福尼亚州帕萨迪纳，建于 1936 年。目前负责 NASA 的无人飞行计划和深空探测计划。

程执行官, 必须保证运载火箭、空间飞行器和使用放射性物质系统的基本设计可以提供对公众、环境和用户的保护措施, 以使放射源泄漏带来的放射性危害达到尽可能低的合理水平。对核安全的考虑必须贯穿项目起自 A 前阶段(概念探索阶段)的各个阶段, 以确保整个使命任务的放射性风险处于可接受的范围内。必须辨识和分析所有包含或使用放射性物质的空间飞行设备(包括医学和其他实验设备)的放射性危险。对核原料计划发射带来的潜在风险, 必须开发详细的地面操作技术规程和放射性意外事故应急方案。作为国家应急计划中所要求的, 意外事故应急计划要包含应急响应措施, 以及恢复工作的保障措施。NPR8710.1《紧急情况应急计划》和 NPR8715.2《NASA 紧急情况应急计划程序需求-修订版》详细描述了 NASA 的紧急情况应急策略和工程需求。

7.5.3 行星保护

美国是联合国和平开发和使用外太空活动控制原则条约的签署国(外太空包括月球和其他天体)。这个外太空条约第九条规定: 对月球和其他天体的探索要遵从“避免对其有害的污染, 避免因外太空物质的引入而导致对地球环境的不利改变。” NASA 的政策(NPD8020.7《飞往和来自外太空的生物污染控制》)规定保护太阳系环境的目的是未来对生物和有机组织的探索。这项 NASA 政策还制定了 NASA 保护地球及其生物圈不受其他行星和外太空星球资源污染的基本策略。NPD 8020.12《无人外太空使命任务中行星保护》规定了 NASA 太空飞行项目必须遵循的一般性规则。根据确定的飞行目标或遭遇的太阳系星球, 根据飞行器或使命任务类型(飞越、轨道器、登陆车、携带样本返回等), 不同使命任务有不同需求。对于某些星体(如太阳、月球、水星), 有最低保护要求。当前对飞往火星和木卫二探测器使命任务的需求则特别严格。表 7.5-1 列举了当前的行星保护策略, 表 7.5-2 简要描述了与它们相关的保护需求。

表 7.5-1 星球保护使命任务种类

行星等级	使命任务类型	分类	实例
直接目的不在于了解星球化学演化, 对此类行星没有任何保护规定(无需求)	任何	I	月球使命
对星球化学演化有明显的兴趣, 但飞行器带来的污染对未来的探索造成危害的概率很小	任何	II	星尘号飞船(飞往) 起源号飞船(飞往) 卡西尼号飞船
对星球的化学演化和生命起源有明显的兴趣, 同时科学观点表明飞行器带来的污染对未来生物实验危害概率可观	飞越, 轨道器	III	奥德赛号飞船 火星全球勘探者 火星勘察轨道器
	登陆车、探测器	IV	凤凰号火星探测漫步器 木卫二探测器 携带火星样本返回(飞往)
太阳系内任何天体	无限制地球返回 ^①	V	星尘号飞船(返回) 起源号飞船(返回)
	有限制地球返回 ^②	V	带回火星样本(返回)
① 对携带回地球的物质/样本不需要特别防护措施;			
② 对携带回地球的物质/样本需要采取特别防护措施, 参见 NPR 8020.12。			

表 7.5-2 星球保护需求概要

任 务 种 类	概 要 需 求
I	分类验证
II	避免空间飞行器和运载火箭意外事故的影响。发射硬件的最终安排归档
III	严格限制产生影响的可能性。对飞行器在轨寿命的要求或无微生物的清洁需求
IV	严格限制产生影响或目标污染的可能性。通过生物鉴定保证着陆器表面的无微生物清洁水平
V	根据目标星球着陆使命任务确定飞往要求。对返回地球使命任务的详细限制依赖于多种因素，但大致包含对接触过目标星球的任何硬件在返回地球之前进行杀菌处理，控制任何带回地球的样本

行星保护是项目管理职责和系统工程活动的核心之一。这项工作与工作分解结构中的多个部分相抵触，而且在早期规划阶段如果不能采纳一个切实可行的行星保护方案，将会增加使命任务的费用和复杂性。行星保护计划在阶段 A 开始规划，在此阶段必须确立使命任务的可行性。在阶段 A 结束之前，项目负责人必须发函到行星保护办公室，陈述使命任务的类型和星际航行目标，请求获得使命任务的行星保护分类。

在阶段 B 结束时的初步设计评审之前，项目负责人必须向 NASA 行星保护办公室提交一个星球保护计划，详细说明为满足要求而采取的行动。这些要求完成的进度要写在发射前行星保护报告中，提交给 NASA 行星保护办公室以获得批准。飞行准备状态评审对这个报告的批准是项目行星保护方案最终批准书的一部分，是获得发射许可所必须的。该报告的更新版本，发射后行星保护报告，应报告实际发射和使命飞行早期出现的事件引起的与计划的使命任务不一致之处。对于要采集样本返回的任务使命，在启动返回地球前，在进入地球再入轨道前，以及在将外太空样本移交给科学团体进行研究之前，需要提交附加的报告和评审。最终，在正式宣布使命任务结束时，需要提交使命任务结束阶段行星保护报告，对比初始的行星保护计划，评审任务使命过程中符合 NASA 行星保护要求的程度并归档化。该文档一般由 NASA 行星保护办公室在国际空间研究委员会（COSPAR）会议上进行报告，向其他空间探索国家通报 NASA 遵循国际行星保护要求的情况。

7.5.4 空间资产设施保护

2001 年 9 月 11 日针对纽约世界贸易中心和五角大楼的恐怖袭击促使美国提高警惕并加强对政府机构的安全保护力度，以确保政府机构的人员、物理设施及信息等资产，尤其是对美国政治、经济和军事能力有重大影响的资产具有足够安全性。当前技术的发展趋势、空间的可达性、空间工程和工业的全球化、空间系统和服务的商业化，以及国际上对美国空间系统的认知，都增加了美国空间系统尤其是其薄弱部分遭受攻击的可能性。限制和阻止自由造访空间的能力和空间作战的能力已不再局限于全球军事力量。实际情况是已经出现许多阻止、干扰甚至物理摧毁空间飞行器及其指挥控制地面设施的能力。关于美国空间系统的功能、位置、物理特性，以及空间作战方法的信息已经越来越多地在国际市场上泄露。敌视美国的国家或组织已经拥有或者能够获得干扰和摧毁美国空间系统的手段，包括攻击在轨卫星、攻击卫星的地面或空间通信节点、攻击卫星指挥和数据处理的地面节点，以及攻击支持空间系统作战的商业基础设施。

7.5.4.1 保护政策

2006 年 8 月 31 日美国总统签发的新的国家空间政策指出,空间能力与国家利益息息相关,美国将“采取必要的行动来保护其空间能力”。同时,在新政策中,还将空间态势感知的责任赋予国防部长。在此授权下,国防部长负责管理民用空间活动和空间作战能力的空间态势感知,尤其是载人空间飞行活动的空间态势感知。空间态势感知提供了关于敌对势力,以及环境对美国、美国盟友及其空间合作系统构成威胁的深度认识和了解,是开发和部署保护措施的重要基础。因此,NASA 空间资产设施的保护同样需要国防部空间态势感知的支持。

7.5.4.2 目标

NASA 的全面空间资产设施保护的目標是,通过缩减和降低与风险相关的、受财政约束的易损性和脆弱性,保证对持久使命任务的支持。

7.5.4.3 范围

空间资产设施保护涉及保护措施的制定和实施,以保护 NASA 的空间资产设施免受有意或无意的,无论是自然还是人为的干扰、阻断和攻击。重要的是,需要对空间系统的所有部分(地面、通信、信息、空间和发射)提供保护,保护措施应覆盖项目的全寿命周期。空间资产设施保护包括人员、物理、信息、通信、信息技术、运行安全,以及反间谍活动等各个方面。系统工程师的作用是将安全能力与空间系统工程和系统运行经验集成起来,按照 NPR8705.4《NASA 有效载荷风险分类》定义的有效载荷分类,开发相应的使命任务保护策略。

7.5.4.4 保护计划

系统工程师利用保护计划流程及其产品(包括工程技术权衡研究和费用效益分析)来满足 NASA 获取、部署和维持安全无害的空间系统。项目保护计划是整理集成相关保护措施的独特文档,防止敏感工程信息的泄露。保护计划为项目管理人员(项目负责人、项目科学家、使命系统工程师、操作管理员、用户团体等)提供对空间系统可能遭受威胁(包括敌对方和环境带来的威胁)的全面认识,发现基础设施的薄弱环节,提出安全对策降低风险和增强使命任务安全性。典型的保护规划概要参见附录 Q。

7.6 公制度量单位的使用

决定一个项目或工程是否采用国际单位制,或公制度量系统,需要考虑多种因素,包括费用、技术、风险和其他一些工程方面问题。

1975 年的度量衡转化法案(公共法案 94-168),以及 1988 年修正的综合贸易和竞争法案(公共法案 100~418),确定了建立公制度量系统作为美国贸易和商业领域重量和尺寸的首选度量衡系统的目标。NASA 制定 NPD8010.2《国际标准度量衡在 NASA 工程中的使用》,用于推行国际标准度量衡并提出 NASA 的特殊要求和责任。

然而,另一个需要考虑的因素是在实施过程中可能有例外的情况。因为全部使用国际标

准单位可能有困难，行政法令《联邦政府工程中的度量衡使用》(EO 12770) 和 NPD 8010.2 都支持意外处理并允许使用“混合”的度量单位。对以下因素的考虑可能直接影响到工程和项目意外处理的实施和应用。

工程或项目必须在寿命周期的早期进行分析，在开发设计方案时需确定何处国际标准单位可行并推荐使用，何处需要使用国际标准单位以外的度量单位。需要考虑的一个主要因素是实际生产的能力或提供基于度量衡的硬件组件能力。分析结果和建议必须提交系统标准评审并得到认可。

在规划项目或工程的实施以生产基于度量衡的系统时，需要考虑的问题如下所述。

- **与原有基于英制单位建造的元件（如电子管，点火装置）的接口：**
 - 是需要从英制单位转换到公制单位，还是需要开发与基于英制的硬件之间的接口。
 - 设计团队应该评审设计实施方案，确保与原有硬件无认证冲突，或者确定并计划需要重新认证的工作。
- **尺寸和公差：**
 - 导致部件互相不匹配。
 - 在度量单位之间转换时出现舍入误差。
 - 当进行单位转换时，开发团队可能需要特定的附加程序、步骤和质量担保人员。
- **工具：**
 - 不是所有商店都有全套加工工具（如钻头、锥丝、铣刀、铰刀等）。
 - 开发团队需要告知可能的承包商使用国际标准的意图，并获得承包商的潜在影响反馈。
- **扣件和配件：**
 - 高强度扣件的选择和使用受制于度量单位。
 - 按最短交货时间，英制单位的轴承、插脚、活塞杆、套管等容易得到。
 - 开发团队需要确定在所需的时间内可接受的基于公制的扣件可用性。
- **基准文件：**
 - 某些关键的航天基准文件如 MIL-HDBK-5《金属材料性质》中只采用英制，使用时需要进行单位转换。
 - 其他关键基准材料或商用数据库仅采用公制。
 - 如果需要，开发团队应当评审需要用到的基准文件，确保可接受度量单位转换控制。
- **共同的知识：**
 - 很多工程师目前用英制单位思考，描述压力时用 PSI（磅/平方英寸），描述材料强度时用 KSI（千磅/平方英寸），描述公差时用 0.003 英寸等。
 - 然而，事实上，当今时代学校毕业的所有工程师都使用国际单位思考，在使用英制单位（如使用“斯勒格^①”表示质量）方面有困难，随着转换错误不断增加需要进行再培训。
 - 开发团队需要了解其成员项目相关的英制和公制单位知识，并使其获得必要的培训和经验。

① 斯勒格 (slug)：英制质量单位，1 斯勒格=32.2 磅。

- **工业实践：**
 - 一些工业企业专门使用英制单位，有时使用英制单位行业术语。降落伞生产企业即属于此类，例如，“60 磅复合材料编织绳”。
 - 其他工业，特别是国际供应商，通常专门使用公制单位，如“30mm 厚原料棒”。
 - 开发团队需要注意这些特别的情况，确保采购及技术设计和集成能够得到适当控制，以避免误差。
- **工程或项目控制：**开发团队应当在系统工程流程早期考虑，需要什么样的工程风险或项目风险管理控制（如技术状态管理步骤）。其中，直接关心的问题包括采用英制和公制度量体系的系统各单元间各种复杂的转换。

某些 NASA 项目使用两种度量体系，这是 NPD 8010.2 所允许的。例如，火星土壤钻探项目采用基于英制的组件设计和开发相关硬件，而采用国际单位完成对组件的分析。其他小规模的项目也成功应用了类似的方法。

对于更大或更分散的项目或工程，可能需要使用更系统、更完整的风险管理措施来成功实现基于国际单位的系统。这需要建立标准的单位转换因子（如从“磅”到“千克”的转换）和标准的国际单位命名文档。风险管理方面的很多问题可以参见相关文档如国家标准和技术学会的《国际标准单位使用指南》，以及国防部的《标准度量衡的标定和开发指南》。

在联邦政府和航天航空工业基地完全转换到使用公制单位之前，各种 NASA 工程和项目必须针对各种情况逐项说明他们实现使用公制单位的程度。对于每个 NASA 工程和管理团队来说，有责任遵守所有的法律规定和行政法令，尽管这在费用、进度和性能方面可能存在一定程度的风险。

附录 A 缩 略 词

ACS	Attitude Control Systems	姿态控制系统
ACWP	Actual Cost of Work Performed	已完成工作的实际成本
AD ²	Advancement Degree of Difficulty Assessment	技术改进复杂度评估
AHP	Analytic Hierarchy Process	层次分析法
AIAA	American Institute of Aeronautics and Astronautics	美国航空航天学会
AO	Announcement of Opportunity	商机公示
ASME	American Society of Mechanical Engineers	美国机械工程师协会
BAC	Budget at Completion	完工成本预算
BCWP	Budgeted Cost for Work Performed	工作完成预算
BCWS	Budgeted Cost for Work Scheduled	工作计划预算
C&DH	Command and Data Handling	指令与数据处理
CACE	Capability for Accelerated Concurrent Engineering	并行工程增长能力
CAIB	Columbia Accident Investigation Board	哥伦比亚号事故调查委员会
CAM	Control Account Manager or Cost Account Manager	控制账目管理员/成本账目管理员
CCB	Configuration Control Board	技术状态控制委员会
CDR	Critical Design Review	关键设计评审
CE	Concurrent Engineering	并行工程
CERR	Critical Event Readiness Review	关键事件准备状态评审
CI	Configuration Item	状态控制项
CM	Configuration Management	技术状态管理
CMC	Center Management Council	中心管理理事会
CMMI	Capability Maturity Model Integration	能力成熟度模型集成
CMO	Configuration Management Organization	技术状态管理组织
CNSI	Classified National Security Information	涉密国家安全信息
COF	Construction of Facilities	设施建造
CONOPS	Concept of Operations	运行使用构想
COSPAR	Committee on Space Research	空间研究委员会
COTS	Commercial Off the Shelf	商用现货
CPI	Critical Program Information or Cost Performance Index	关键工程信息/费用性能指标
CRM	Continuous Risk Management	持续风险管理
CSA	Configuration Status Accounting	技术状态状况登记
CWBS	Contract Work Breakdown Structure	合同工作分解结构
DCR	Design Certification Review	设计认证评审
DGA	Designated Governing Authority	指定管控机构
DLA	Defense Logistics Agency	国防后勤保障局
DM	Data Management	数据管理

DOD	Department of Defense	国防部
DOE	Department of Energy	能源部
DODAF	DOD Architecture Framework	DOD 架构框架
DR	Decommissioning Review	退役评审
DRM	Design Reference Mission	设计参考使命任务
EAC	Estimate at Completion	完工成本估算
ECP	Engineering Change Proposal	工程技术变更申请
ECR	Environmental Compliance and Restoration or Engineering Change Request	环境合规和复原/ 工程技术变更请求
EEE	Electrical, Electronic, and Electromechanical	电子、电气和电动机
EFFBD	Enhanced Functional Flow Block Diagram	增强功能流框图
EIA	Electronic Industries Alliance	电子工业联合会
EMC	Electromagnetic Compatibility	电磁兼容性
EMI	Electromagnetic Interference	电磁干扰
EMO	Environmental Management Office	环境管理办公室
EO	Executive Order	行政法令
EOM	End of Mission	使命任务结束
EV	Earned Value	挣值
EVM	Earned Value Management	挣值管理
FAD	Formulation Authorization Document	规划论证授权文档
FAR	Federal Acquisition Requirement	联邦采办需求
FCA	Functional Configuration Audit	功能技术状态审核
FDIR	Failure Detection, Isolation, And Recovery	故障检测、定位与修复
FFBD	Functional Flow Block Diagram	功能流框图
FMEA	Failure Modes and Effects Analysis	故障模式与影响分析
FMECA	Failure Modes, Effects, and Criticality Analysis	故障模式、影响与重要度分析
FMR	Financial Management Requirements	财务管理需求
FRR	Flight Readiness Review	飞行准备状态评审
FS&GS	Flight Systems and Ground Support	飞行系统和地面保障
GEO	Geostationary	地球静止轨道
GFP	Government-Furnished Property	政府登记财产
GMIP	Government Mandatory Inspection Point	政府强制检查点
GPS	Global Positioning Satellite	全球定位卫星
HF	Human Factors	人因
HQ	Headquarters	总部
HQ/EMD	NASA Headquarters/Environmental Management Division	NASA 总部/环境管理部
HWIL	Hardware in the Loop	硬件在回路
ICA	Independent Cost Analysis	独立费用分析
ICD	Interface Control Document/Drawing	接口控制文档/图纸
ICE	Independent Cost Estimate	独立费用估算

ICP	Interface Control Plan	接口控制计划
IDD	Interface Definition Document	接口定义文件
IEEE	Institute of Electrical and Electronics Engineers	电子与电气工程师协会
ILS	Integrated Logistics Support	综合后勤保障
INCOSE	International Council on Systems Engineering	国际系统工程协会
INSRP	Interagency Nuclear Safety Review Panel	跨机构核安全特别评审小组
IPT	Integrated Product Team	一体化产品团队
IRD	Interface Requirements Document	接口需求文档
IRN	Interface Revision Notice	接口修订通告
ISO	International Organization for Standardization	国际标准化组织
IT	Information Technology or Iteration	信息技术/迭代
ITA	Internal Task Agreement	内部任务协议
ITAR	International Traffic in Arms Regulation	国际武器交易规章
I&V	Integration and Verification	集成与验证
IV&V	Independent Verification and Validation	独立验证与确认
IWG	Interface Working Group	接口工作小组
JPL	Jet Propulsion Laboratory	喷气推进实验室
KDP	Key Decision Point	关键决策点
KSC	Kennedy Space Center	肯尼迪航天中心
LCCE	Life-Cycle Cost Estimate	寿命周期费用估算
LEO	Low Earth Orbit or Low Earth Orbiting	低地球轨道
LLIL	Limited Life Items List	有限寿命物品清单
LLIS	Lessons Learned Information System	经验总结信息系统
M&S	Modeling and Simulation	建模与仿真
MAUT	Multi-Attribute Utility Theory	多属性效用理论
MCDA	Multi-Criteria Decision Analysis	多准则决策分析
MCR	Mission Concept Review	使命任务概念评审
MDAA	Mission Directorate Associate Administrator	使命任务主管助理
MDR	Mission Definition Review	使命任务定义评审
MOE	Measure of Effectiveness	效能指标
MOP	Measure of Performance	性能指标
MOU	Memorandum of Understanding	谅解备忘录
NASA	National Aeronautics and Space Administration	国家航空航天局
NEDT	NASA Exploration Design Team	NASA 空间开发设计团队
NEPA	National Environmental Policy Act	国家环境政策法案
NFS	NASA FAR Supplement	NASA 联邦采办需求补充
NODIS	NASA On-Line Directives Information System	NASA 在线指令信息系统
NIAT	NASA Integrated Action Team	NASA 一体化行动团队
NOAA	National Oceanic and Atmospheric Administration	国家海洋大气局
NPD	NASA Policy Directive	NASA 政策指令

NPR	NASA Procedural Requirements	NASA 技术规程需求
OCE	Office of the Chief Engineer	总工程师办公室
OGC	Office of the General Counsel	总法律顾问办公室
OMB	Office of Management and Budget	管理与预算办公室
ORR	Operational Readiness Review	运行使用准备状态评审
OSTP	Office of Science and Technology Policy	科学与技术政策办公室
OTS	Off-the-Shelf	现货
PAR	Program Approval Review	工程审批评审
PBS	Product Breakdown Structure	产品分解结构
PCA	Physical Configuration Audit or Program Commitment Agreement	物理技术状态审核/工程承诺协议
PD/NSC	Presidential Directive/National Security Council	总统指令/国家安全署
PDR	Preliminary Design Review	初步设计评审
PERT	Program Evaluation and Review Technique	工程评价与评审技术
PFAR	Post-Flight Assessment Review	飞行后评估评审
PHA	Preliminary Hazard Analysis	初步危险分析
PI	Performance Index/Principal Investigator	性能指标/责任调查员
PIR	Program Implementation Review	工程实施评审
PIRN	Preliminary Interface Revision Notice	初步接口修订通告
PKI	Public Key Infrastructure	公共密钥基础结构
PLAR	Post-Launch Assessment Review	发射后评估评审
P(LOC)	Probability of Loss of Crew	乘员损失概率
P(LOM)	Probability of Loss of Mission	使命任务失败概率
PMC	Program Management Council	工程管理专业组
PPBE	Planning, Programming, Budgeting and Execution	计划、规划、预算与执行
PPO	Planetary Protection Officer	行星保护官员
PQASP	Program/Project Quality Assurance Surveillance Plan	工程/项目质量保证监督计划
PRA	Probabilistic Risk Assessment	概率风险评估
PRD	Project Requirements Document	项目需求文档
PRR	Production Readiness Review	产品准备状态评审
P/SDR	Program/System Definition Review	工程/系统定义评审
PSR	Program Status Review	工程状态评审
P/SRR	Program/System Requirements Review	工程/系统需求评审
PTR	Periodic Technical Reviews	定期技术评审
QA	Quality Assurance	质量保证
R&T	Research and Technology	研究与技术开发
RF	Radio Frequency	无线电
RFA	Requests for Action	行动申请
RFI	Request for Information	信息申请
RFP	Request for Proposal	申请指南
RID	Review Item Discrepancy	评审事项差异

SAR	System Acceptance Review or Safety Analysis Report	系统验收评审/安全性分析报告
SBU	Sensitive But Unclassified	敏感但未定密
SDR	System Definition Review	系统定义评审
SE	Systems Engineering	系统工程
SEE	Single-Event Effects	单个事件影响
SEMP	Systems Engineering Management Plan	系统工程管理计划
SER	Safety Evaluation Report	安全性评价报告
SI	System Internationale (metric system)	国际单位体制(公制)
SIR	System Integration Review	系统集成评审
SMA	Safety and Mission Assurance	安全性和使命任务保证
SOW	Statement of Work	任务书
SP	Special Publication	特别出版物
SPI	Schedule Performance Index	进度性能指标
SRB	Standing Review Board	独立评审委员会
SRD	System Requirements Document	系统需求文档
SRR	System Requirements Review	系统需求评审
SSA	Space Situational Awareness	空间态势感知
STI	Scientific and Technical Information	科学与技术信息
STS	Space Transportation System	空间运输系统
SysML	System Modeling Language	系统建模语言
T&E	Test and Evaluation	试验与评价
TA	Technology Assessment	技术评估
TBD	To Be Determined	待确定
TBR	To Be Resolved	待解决
TDRS	Tracking and Data Relay Satellite	跟踪与数据中继卫星
TDRSS	Tracking and Data Relay Satellite System	跟踪与数据中继卫星系统
TLA	Timeline Analysis	时间控制基线分析
TLS	Timeline Sheet	时间控制基线表
TMA	Technology Maturity Assessment	技术成熟度评估
TPM	Technical Performance Measure	技术性能指标
TRAR	Technology Readiness Assessment Report	技术成熟度评估报告
TRL	Technology Readiness Level	技术成熟度水平
TRR	Test Readiness Review	试验准备状态评审
TVC	Thrust Vector Controller	推力矢量控制
UML	Unified Modeling Language	统一建模语言
USML	United States Munitions List	美国军需品清单
V&V	Verification and Validation	验证与确认
VAC	Variance at Completion	完成时偏差
WBS	Work Breakdown Structure	工作分解结构

附录 B 专用词汇表

条 目	定义/语境
可接受风险 Acceptable Risk	已经被工程/项目的管理机构、使命任务主管和其他客户了解并同意，不再需要进一步专门缩减行动的风险
采办 Acquisition	以适当资金额签订合同，通过购买或租借的方式，获取为政府所用的物资或服务；这些物资或服务可能是现成的，也可能正在进行必要的创建、研发、演示验证和评价。采办开始于 NASA 要求确定的时刻，包括一系列需求的描述（如满足 NASA 要求的需求）、原材料的征集和选择、合同定标、合同筹资、合同执行、合同管理，以及那些与 NASA 通过合同要求的流程直接相关的技术和管理功能
活动 Activity	（1）项目的任何一个阶段或研究工作，在执行时能提交一个产品、服务、保障或可预见的成熟技术。（2）一组任务，用于描述为完成流程并帮助产生期望结果的技术工作
技术改进难度评估 Advancement Degree of Difficulty Assessment (AD ²)	对促进系统成熟度水平需要什么形成了解的过程
配定控制基线（阶段 C） Allocated Baseline (Phase C)	配定控制基线是已批准的为状态控制项开发的面向性能的技术状态文档，该文档描述从更高层次需求文件或状态控制项分配的功能和接口特性，并描述为验证这些特性要求是否达到需要进行的演示验证。配定控制基线是对功能控制基线的顶层性能要求的扩展，补充了着手进行状态控制项制造和编码的细节。配定控制基线在初步设计评审时确定，由 NASA 控制。配定控制基线的控制通常紧随功能技术状态审核发生
分析 Analysis	基于计算数据和来自低阶系统结构目标产品确认的数据，运用数学模型和解析技巧预测系统设计与需求的符合程度
备选方案分析 Analysis of Alternatives	比较备选方案的正式分析方法，通过效能分析评估满足使命任务需求能力和通过费用分析评估寿命周期费用。两个分析结果结合形成费效比，使得决策者能够评定各备选方案的相对价值和潜在的工程性回报
层次分析法 Analytic Hierarchy Process	一种经过验证并有效的处理复杂决策问题的多属性评定方法，能够辅助对评定标准的辨识和赋权，辅助分析针对评定标准收集的数据，并加快决策过程
审批 Approval	相关管理官员授权进行所提议的系列行动。审批过程必须归档
（实施执行）审批 Approval (for Implementation)	决策机关认可，工程/项目符合相关利益者的期望和规划论证需求，并已准备就绪可推进实施。通过批准工程/项目，决策机关承诺进入实施阶段所需要的经费和资源预算
已部署控制基线 As-Deployed Baseline	已部署控制基线发生在运行使用准备状态评审时，在此时刻系统设计被认为在功能上实现了飞行准备。所有变更将写入技术文档
控制基线 Baseline	一个各方同意的需求、设计或文档集合，通过正式的审批和监控流程保证系统变更能够受控
双向可追溯性 Bidirectional Traceability	两个或多个逻辑实体之间的关联，这种关联可以在每个方向（即在指向和离开实体的方向）上辨识
硬试样 Brassboard	系统研究的一种构形，适合外场试验。它复现系统运行使用的实际功能和技术状态，但不考虑系统非本质的方面因素，如包装
软试样 Breadboard	系统研究的一种构形，通常不适合外场试验。它复现系统运行使用的实际功能，但不需复现其实际技术状态，而且与系统的实际物理布局有很大区别
分属设施 Component Facilities	隶属于 NASA 中心或机构的但在地理上分离的综合设施

续表

条 目	定义/语境
运行使用构想 Concept of Operations (ConOps)	运行使用构想描述系统在寿命周期各阶段如何使用以达到利益相关者的期望。它从运行使用的视角描述系统特性并促进对系统目标的理解。它激发与系统用户单元相关的系统需求和体系结构的开发。它是后续各类定义文档的基础并为长远的运行使用规划活动提供基础
同意书 Concurrence	管理官员关于接受行动方案建议的书面同意书
并行工程 Concurrent Engineering	以并行工程模式而非串行工程模式进行的设计
状态控制项 Configuration Items	状态控制项是用于进行相应技术状态管理的能够满足最终使用功能的硬件、软件，或两者的组合。状态控制项通常用文字和数字标识，这种标识同样可以用来作为状态控制项中独立可辨识单元的标识序号
技术状态管理流程 Configuration Management Process	将管理科学应用到产品寿命周期中，用于控制产品的性能方面、功能方面和物理方面特性的变更并为这类控制提供直观性。它确保产品的技术状态可知并反映在产品的信息中，保证产品变更是有益的且没有相反结果的影响，并保证变更是可控的
相关背景图 Context Diagram	外部系统对所设计系统影响的图示说明
持续风险管理 Continuous Risk Management	完善风险管理手段的迭代过程。该过程的步骤包括风险分析、风险跟踪与控制手段规划、风险跟踪、风险控制实施、所有风险信息的归档与交流，以及全过程中为完善该过程进行的研讨
合同 Contract	一种相互制约的法律关系，要求供货方提供货物和服务（包括组装），并要求购货方为此支付费用。合同以书面形式（除非有其他形式的授权）明确政府拨款对应的所有条件和承诺
承包商 Contractor	由个人、合伙人、商号、公司、协会或其他行业与 NASA 就某项工程或项目签订合同，按照合同要求进行相应产品的设计、研发、制造、维护、更新、运行和保障工作，或根据合同要求提供相应服务
控制账目管理员 Control Account Manager	在工作分解结构中 with 子系统对应的控制账目层，负责控制账目偏差的官员。合同账目管理员负责制定工作和生产进度计划、分阶段资源调度计划。通常子系统的技术负责人/指挥担任此角色，作为其子系统管理责任的一部分
控制门（里程碑） Control Gate (or milestone)	参见“关键决策点”
费用效益分析 Cost-Benefit Analysis	通过对比等价费用或等价效益来确定各备选方案之间优劣的方法。它需要考虑全部正面因素和负面因素来确定最终结果
费用效能分析 Cost-Effectiveness Analysis	对比达到特定目标等价效益的各备选方案费用的系统定量分析方法
关键设计评审 Critical Design Review	该评审用于证明设计成熟度已经适应于支持系统全尺寸的制造、组装、集成和试验，技术成果已经能够完成飞行和地面系统的研发与任务执行，保证在给定的费用和进度约束下达到任务的性能需求
关键事件 Critical Event (key event)	在项目规划的产品全寿命周期中需要监控的事件，该类事件可能产生影响系统设计、研发、制造、试验和运行的关键需求（如在效能、性能和技术能力方面）
关键事件准备状态评审 Critical Event Readiness Review	该评审确认项目在飞行任务中执行关键活动的准备状态

续表

条 目	定义/语境
客户 Customer	申请产品并将收到交货的组织或个人。客户可能是产品的最终用户、产品最终用户的采办代理或某项技术成果中间产品的需求者。系统层的每个产品都有其客户
数据管理 Data Management	数据管理用于规划、获取、访问、管理、保护和运用技术特性数据来支持系统的全寿命周期
决策分析流程 Decision Analysis Process	该流程给出进行决策的方法论。它提供决策问题的数学建模方法并用于找到最优决策的数值解。该方法需要辨识作为决策依据的方案，需要产生顺序发生的可能事件，需要获得来自于决策和事件组合的输出结果
决策机构 Decision Authority	能够在关键决策点授权工程/项目转入下一寿命周期阶段的 NASA 责任单位
决策矩阵 Decision Matrix	一种评价备选方案的方法。该方法中评价准则通常放在矩阵的最左侧一列，备选方案放在矩阵最上方一行。通常需要对每一个评价准则赋予“权重”
决策支撑资料 Decision Support Package	与正式评审和变更请求结合形成的提交决策评审的文档
决策树 Decision Trees	一个图示的决策模型，该模型建立各个备选方案期望结果对应的所有节点，在此基础上通过适当赋权计算所有方案的可能结果
退役评审 Decommissioning Review	该评审确认系统终止和退役的决定，并评估系统资产安全退役和处置的准备状态。退役评审通常在系统达到规划任务目标的基础上接近执行例行任务的结束时进行。它可能在偶然事件引起任务过早终止时提前进行，也可能在需要附加研究而延长任务周期时推迟进行
可交付数据产品 Deliverable Data Item	包括技术层面数据需求规范、设计文档、管理数据计划和度量标准报告
演示验证 Demonstration	通过运行使用已实现的目标产品表明利益相关者的一系列期望已经达到
派生需求 Derived Requirements	对于一项工程，指需要满足工程主管要求的那些需求。 对于一个项目，指需要满足项目工程要求的那些需求
溢出范围 Descope	超出项目的范围
设计方案定义流程 Design Solution Definition Process	将根据利益相关者的期望和逻辑分解过程得到的高层需求转变为设计解决方案的过程
政府主管机构 Designated Governing Authority	在工程、项目、活动以上层次具有技术监督责任的管理实体
逐步细化法 Doctrine of Successive Refinement	由利益相关者的期望驱动的回归与迭代设计过程，其中需要开发系统初步架构/设计，相关运行使用构想和派生需求
挣值 Earned Value	在给定的进度时刻，（已完成或进行中）的产品实际完成的任务和生产相应预算费用的总和
挣值管理 Earned Value Management	在项目执行过程中，通过技术与进度和费用目标的集成来度量和评估项目状况的工具。挣值管理提供技术进步的量化，能够洞察项目的状态和项目完成时的费用和进度。挣值管理成功的两个基本特征是挣值管理系统数据完整性和精心确定目标的挣值管理每月数据分析（即有风险的工作分解结构单元）
辅助产品 Enabling Products	为目标产品的全寿命周期运行和使用提供保障的产品和服务（如生产、试验、部署、训练、维护和处置）。目标产品和它的辅助产品是相互独立的，共同看做一个系统。这样，项目的职责就扩展到了在产品寿命周期的每个阶段从相关的辅助产品中获取服务。当不存在合适的辅助产品时，项目应为所负责的目标产品创建并使用其辅助产品

续表

条 目	定义/语境
技术成本估算 Technical Cost Estimate	项目技术工作的成本估算, 由项目技术团队依据他们对系统需求和运行使用构想的理解及对系统结构的认识实施
扩展功能流框图 Enhanced Functional Flow Block Diagram	能够同时表示系统功能流、控制流和数据流的框图
启动准则 Entry Criteria	每个项目进入下一寿命周期阶段或技术成熟度水平所需达到的最小成果
环境影响 Environmental Impact	一个行动对环境造成的直接的、间接的或累积的有益或有害影响
环境管理 Environmental Management	保证工程和项目的行动和决策对环境可能的影响在论证规划阶段被评估, 以及在系统实现流程中反复评价的活动。这个活动的实施必须遵从所有 NASA 政策及联邦、各州和地方环境法律和规章
(相关流程) 章程 Establish (with respect to processes)	为实施流程活动制定的开发政策、工作指导和技术规程的法令
评价 Evaluation	不间断的独立的(即工程/项目支持者以外的)对工程或项目状况的评价, 以及根据评价结果确认依据规划实施和执行计划的适当性
扩展性 Extensibility	一项决策扩展到其他应用的能力
灵活性 Flexibility	一项决策支持当前应用以外多项应用的能力
飞行准备状态评审 Flight Readiness Review	该评审检查试验、演示验证、分析和审核结果, 确定系统的准备状态已能够达到安全和成功的起飞/发射和执行后续飞行任务的要求。它同时保证所有飞行和地面相关硬件、软件、人员和程序已经准备就绪
飞行系统和地面保障 Flight Systems and Ground Support	飞行系统和地面保障是 NASA 四个相互关联的产品系列之一。飞行系统和地面保障项目导致最复杂最可观的 NASA 投资。为了管理这些系统, 飞行系统和地面保障项目的论证和实施阶段与 NASA 项目寿命周期有相同的模型, 从阶段 A (概念开发) 到阶段 F (退役处置)。开展飞行系统和地面保障项目的主要动因是安全性和任务成功
浮动时间 Float	进度计划内的额外时间
规划论证阶段 Formulation Phase	定义在 NPR 7120.5 中的 NASA 管理寿命周期的第一部分。在该阶段中, 系统需求控制基线被明确、系统可行概念被确定、系统定义的控制基线根据选定的概念被明确, 并准备进入系统实施阶段
功能分析 Functional Analysis	辨识、描述和关联系统为达到其目的和目标必须实现的功能的过程
功能控制基线 (阶段 B) Functional Baseline (Phase B)	功能控制基线是一个被批准的系统技术状态文档, 其描述系统或顶层状态控制项的(功能上、互操作性和接口特性)性能需求, 以及演示执行这些特性已实现所需进行的验证
功能技术状态审核 Functional Configuration Audit (FCA)	检查成形产品的功能特性, 通过试验结果验证产品满足在其功能控制基线文档中指定的需求, 该文档在初步设计评审和关键设计评审中获得批准。功能技术状态审核将在硬件成形产品和软件成形产品上实施, 并在成形产品的物理技术状态审核之前实施
功能分解 Functional Decomposition	在设计方案定义和功能逻辑分解下获得的分系统功能。通过考察系统功能来辨识为实现系统功能及功能之间的关系和接口所需要的分系统功能

续表

条 目	定义/语境
功能流框图 Functional Flow Block Diagram	用于定义系统功能及功能事件时序的框图
甘特图 Gantt Chart	在工作分解结构中描述活动和产品起始和结束日期的条状图
目的 Goal	对诸如性能准则、技术差距、系统相关背景、效能、费用、进度和风险等的定量和定性说明
政府强制检查点 Government Mandatory Inspection Points	联邦法规所确定的检查点, 为了保证系统完全服从安全性和任务关键属性要求。如果不符合这些要求将导致任务失败和人员损失
固有能力 Heritage (or legacy)	指制造商固有的质量和可靠性水平, 通过以下作为传统能力一部分的指标验证: (1) 服务时间; (2) 服务单元数量; (3) 平均无故障时间; (4) 使用周期的数量
人因工程 Human Factors Engineering	研究人类与系统接口的学科, 提出需求、标准和指南以保证作为集成系统一部分的人类能够承担预期的功能
实施执行阶段 Implementation Phase	定义在 NPR 7120.5 中的 NASA 管理寿命周期的一部分。该阶段完成系统产品的详细设计, 完成待部署产品的建造、组装、集成和试验, 根据使用和任务要求完成产品到客户/用户的部署
不可预计费 Incommensurable Costs	不易度量的费用, 如控制发射造成的污染和减少残骸碎片
影响图 Influence Diagram	决策状态的一个紧密的图形和数学表达
检查 Inspection	对已实现的目标产品的表面检查, 以确认产品的物理设计特征或指定生产商的标识
综合后勤保障 Integrated Logistics Support	在系统工程流程的集成(阶段 D)和运行(阶段 E)中以最佳效益的方式为产品系统提供保障的活动。这些活动是预先完成的, 包括早期的并行考虑保障性特性, 实施系统可选方案与综合后勤保障概念的权衡研究, 运用优化方法量化每个综合后勤保障单元的资源需求, 以及获取每个综合后勤保障单元的保障物品
接口管理流程 Interface Management Process	当项目计划分解到参与单位(如政府、承包商、地理上分布的技术团队)时辅助进行产品开发控制的过程, 以及(或)定义并维护需要互操作的产品一致性的过程
迭代 Iterative	针对同一产品或一组产品出现的需求变更或差异进行修正的应用过程(参见“递归”和“可再现”)
关键决策点(或里程碑) Key Decision Point (or milestone)	决策机构确定工程/项目已经具备推进到寿命周期下一阶段(或下一关键决策点)的时刻点
知识管理 Knowledge Management	在正确的时间将正确的信息无延迟传达到正确的人员, 帮助人员形成并共享知识, 且以正确的方式采取行动, 从而明显地改善 NASA 及其合作伙伴的行为能力
最小费用分析 Least-Cost Analysis	辨识满足项目技术需求的费用最小的项目方案选择方法
留置 Liens	需求和任务未能满足, 项目必须在一个给定的时间内解决问题并通过控制节点向前推进
寿命周期费用 Life-Cycle Cost	项目或系统寿命周期中(从规划论证到实施执行)发生的全部费用, 包括在项目的设计、研发、验证、生产、部署、运用、维护、保障和处置过程中的全部直接和间接费用、重复和非重复费用, 以及其他已发生的相关费用和估计将发生的费用

续表

条 目	定义/语境
逻辑分解模型 Logical Decomposition Models	采用一种或多种方法（如功能、时间、行为、数据流、状态、模式、系统结构）对需求进行分解
逻辑分解流程 Logical Decomposition Process	生成详细功能需求使得 NASA 工程和项目能够满足利益相关者最终需要的过程。该流程辨识系统在各个层次上必须达到的要求，从而保证项目成功。它运用功能分析法生成系统结构，并将系统顶层需求逐层分解，直到分解到项目所需要的最低层次
后勤保障 Logistics	与空间飞行和地面系统保障性目标所确认的设计需求定义、材料获取和分配、维护保养、备件更换、运输和处置相关的管理、工程、分析等活动
维护（与建立流程相关） Maintain (with respect to establishment of processes)	进行流程计划、资源供给、责任划分、人员训练、技术状态管理、利益相关者辨识和参与、流程效果监控等相关行动
维修性 Maintainability	由具有特定技术水平的人员使用规定的程序和资源在规定的维修水平上进行维修，从而使一个物品保持或恢复指定条件这种能力的度量
余量 Margin	考虑到不确定性和风险而在预算、项目进度、技术性参数（如重量、能源、内存）中加入的补充。余量在规划论证过程中基于风险的评估确定分配控制基线，并且通常在工程/项目的全寿命周期中耗费
效能指标 Measure of Effectiveness	通过评估生产和提交的产品或系统相关技术成果，判断利益相关者的期望是否满足的度量指标。效能指标不仅是产品被利益相关者所接受的关键度量指标，而且是用于运行和执行使命任务的关键度量指标。效能指标通常是产品质量的定性指标，而不能直接用于作为设计需求
性能指标 Measure of Performance	当设计完成时，用于确定产品或系统的效能指标能够满足要求的定量度量指标。在设计过程中，性能指标受到特别关注，以使它们对应的效能指标能够满足。每个效能指标通常有两个或更多性能指标与之对应
指标（体系） Metric	针对系统、流程和活动的状态或性能的重要信息，在一段时间内进行度量的结果。指标可以引导适当的行动
使命任务 Mission	为实现 NASA 的目标或有效地创造与 NASA 目标直接相关的科学、技术、工程条件而进行的主要活动。使命任务需求不受任何特定的系统和技术解决方案的影响
使命任务概念评审 Mission Concept Review	为认证使命任务需求并考核所提出的使命任务目标及实现使命任务目标的构想而进行的评审。这是一项系统研发组织的内部评审
使命任务定义评审 Mission Definition Review	为考核所定义的系统功能和性能需求及初始工程/项目方案，并保证这些需求和选定的构想满足使命任务需要而进行的评审
NASA 寿命周期阶段（工程寿命周期阶段） NASA Life-Cycle Phases (or program life-cycle phases)	由 NPR7120.5 定义的规划论证阶段和实施执行阶段组成
目标函数（某些情况下为费用函数） Objective Function (sometimes Cost Function)	将可能结果的组合值表示为单一费效指标的数学表达式
运行使用准备状态评审 Operational Readiness Review	用于考核实际系统特征及系统或产品运行使用的技术规程，并确保所有系统和（飞行、地面）保障硬件、软件、人员、技术规程、用户文档能精确反映系统的部署状态而进行的评审
Optimal Solution 最优解决方案	达到目标函数最小值（或最大值，当以此为目标时）的可行解决方案

续表

条 目	定义/语境
其他关注团体（利益相关者） Other Interested Parties (Stakeholders)	利益相关者的一个子集，是指那些不是所计划技术成果的客户，但可能被目标产品及其实现和使用方式所影响，或有责任提供寿命周期保障服务的组织和个人
同行评审 Peer Review	内部或外部的领域专家进行的独立评价，这些专家在被评审的产品上没有既得利益。同行评审可以是针对选定的未完成产品进行的有计划的专门评审，用于在该产品进入里程碑评审或审批环节之前辨识其存在的瑕疵和问题
性能指标 Performance Index	备选方案的综合效果度量
性能标准 Performance Standards	用于性能标准（包括费用和进度）的公共度量衡
物理技术状态审核（技术状态检查） Physical Configuration Audits (or configuration inspection)	物理技术状态审核考核设定产品的物理技术状态，并验证该产品是否与已在关键设计评审批准的产品控制基线文件相对应物理技术状态审核对于设定的硬件和软件都需要进行。
飞行后评估评审 Post-Flight Assessment Review	用于评价飞行活动结束后为下一次飞行任务而进行的评审。该评审辨识在飞行和任务期间的所有异常，并确定在未来飞行中减缓或消除这些异常所应采取的行动
发射后评估评审 Post-Launch Assessment Review	用于评价基于发射后飞行和运行使用经历的项目状态、性能和能力进行的评审，这也意味着对责任从开发商转换到运行商的准备状态进行评估。该评审还评价项目计划的状态及其完成重点在于近期运行使用和任务关键事件上的使命任务能力。该评审通常在飞行运行使用早期和初步检查后进行
顺序图 Precedence Diagram	将活动置入方框并用归属箭头相连的工作流程图，是甘特图的特例
初步设计评审 Preliminary Design Review	用于验证初步设计在可接受的风险条件下和费用进度约束下已达到系统需求，并建立进行详细设计的基础而进行的评审。它将说明设计选择了正确方案，接口已经明确，验证方法已经描述
流程 Process	用于将输入转换成所需要输出的一系列活动，目的是形成所期望的满足目标的结果
可生产性 Producibility	系统在便利和经济方面的特征，由此可以实现将完整的设计（通过组装、制造、编码）转换为硬件和/或软件
产品 Product	系统的一部分，包括目标产品，能够履行运行功能并能够使产品执行寿命周期服务，这些服务与目标产品或以某种形式的未完成产品（如计划、控制基线或试验结果）形式存在的技术成果相关
产品控制基线（阶段 D/E） Product Baseline (Phase D/E)	产品控制基线是一类被批准的技术文档，该文档描述在寿命周期的生产、部署和运行保障阶段，一个状态控制项的内容。产品控制基线描述状态控制项的物理属性或外形、尺寸和功能的详细特征，描述生产验收试验选定的功能特征，描述生产验收试验的需求
产品分解结构 Product Breakdown Structure	工程/项目硬件和软件产品的层次化分解
产品实施流程 Product Implementation Process	在启动系统工程引擎自底向上到产品交付流程的活动中遇到的第一个流程。在此流程中将产品的计划、设计、分析、需求开发和图纸实现为真实的产品
产品集成流程 Product Integration Process	构成系统结构的产品实现途径之一。在此过程中，低层的产品组装成高层产品，同时检验确保集成的产品有正确的功能。它是产品实施流程和验证确认流程之间，将低层实现的产品引入高层目标产品的一系列流程中的第一个

续表

条 目	定义/语境
产品实现 Product Realization	制造、购买或重用一个产品的行动，或是将低层实现产品组装和集成为新产品，验证和确认产品满足其相应需求，并将产品交付到客户的行动
产品交付流程 Product Transition Process	向客户交付经过验证和确认的通过产品实施或产品集成形成的目标产品的流程，目的是集成系统结构上一层次目标产品或集成向最终用户提交的顶层目标产品
产品确认流程 Product Validation Process	针对实际目标产品的验证和确认流程的第二阶段。验证流程证明“系统实现过程是正确的”，而确认流程证明“实现的是正确系统”。换句话说，验证提供每一个“需要”形式陈述的需求都已实现的依据，而确认向客户和用户展示在指定的运行环境中系统功能以期望的形式得到保证。这一点通过在系统结构的每个层次上检查产品来完成
产品验证流程 Product Verification Process	针对实际目标产品的验证和确认流程的第一阶段。该流程应用于系统工程通用技术流程中，证明通过产品实施流程或产品集成流程提交的实际产品是以满足寿命周期阶段成功准则的适当形式实现的
产品准备状态评审 Production Readiness Review	当飞行系统和地面系统项目需要开发或采办多个系统或不少于三个（或项目指定）相近系统时进行的评审。产品成熟度评审决定系统开发者是否已准备就绪，以有效地生产所需要数量的系统。它确保生产计划，基于建造、组装和集成的产品，以及生产人员已经准备就绪可开始产品生产
工程 Program	一项由使命任务主管部门（或使命任务保障办公室）负责的战略投资，需确定工程目的、目标、结构、资金和管理结构，以支持一个或多个项目的进行
工程/系统定义评审 Program/System Definition Review	该评审检查所提议工程的结构及直到系统功能单元的分解，对所提议工程的目标和实现这些目标的概念进行评价，对关键技术和其他风险进行辨识和评估。该评审给出计划的方案、预算和进度控制基线
工程/系统需求评审 Program/System Requirements Review	该评审用于确保工程的需求得到适当确切的阐述，并且符合 NASA 和使命任务主管部门的战略目标
工程性需求 Programmatic Requirements	可能情况下，相应由任务主管部门、工程、项目和性能指标确定的需求。这些需求包括战略的科学和探索需求、系统性能需求，以及进度、费用和其他类似的非技术约束
项目 Project	（1）规定了目的、目标、需求、寿命周期费用、起始和终止时刻的特定的投资。一个项目产生新的或改进的直接遵从 NASA 战略需要的产品或服务。这些产品或服务可以完全是内部的，也可以是提供给政府、工业部门和学术伙伴的，也可以通过合同方式提供给私人企业。（2）在工程、项目和活动中所开展的工作
项目计划 Project Plan	建立项目实施控制基线的文档，根据需要由工程负责人、中心主任、项目负责人和任务主管部门相关负责人签署
项目技术团队 Project Technical Team	参与项目开发的全部技术团队
招商文件 Solicitation	承包商为承揽产品或服务合同的申请资料载体
原型 Prototype	寿命周期早期制造的物品（样机、模型），在外形、尺寸和功能上与实际飞行构件相近，以表明在当时研发阶段的可行性。原型用于反映设计解决方案以便从原型中获得的经验能够反馈到设计变更中，从而提升单一飞行构件或由若干飞行构件构成的产品的制造、集成和维修性
质量保证 Quality Assurance	为确信实际产品是依据其功能、性能和设计需求生产和部署的而需要进行的独立评估

续表

条 目	定义/语境
已实现产品 Realized Product	经四个产品实现流程应用输出的所需要结果。产品的形式依赖于相关产品寿命周期的阶段和该阶段的成功准则
递归 Recursive	为了在系统结构中设计更低层次的系统产品或实现更高层次的目标产品，通过流程的重复应用为系统增加附加价值。同时也是将同一流程重复应用到系统结构的寿命周期下一阶段，以便提高系统定义成熟度并满足该阶段完成准则
相关利益者 Relevant Stakeholder	参见“利益相关者”
可靠性 Reliability	系统在期望的寿命中通过正确执行功能保证任务成功程度的度量。系统有一个最低的和可接受的故障（失效）概率，可靠性通过对可靠部件和材料的简化，以及适当设计和合理应用获得。除了长寿命之外，一个可靠的系统还应当是健壮的和容错的
可再现 Repeatable	流程的特性，能够应用于产品系统结构的任意层次或任意寿命周期阶段
需求 Requirement	经过商定的以“需要”形式阐述的对需要、期望、要求、能力的描述，以及对人力、设备、设施或其他资源和服务的需求，在特定的时期或特定的时刻的定量描述。可接受的需求阐述形式应当是清晰的、正确的、可行的、无歧义的，并且能够在所指定的系统结构层次上被确认。在同一组需求阐述中，他们应当是不冗余的、适当关联的、互不冲突的
需求分配表单 Requirements Allocation Sheet	描述功能分配、性能分配和物理系统关联关系的文档
需求管理流程 Requirements Management Process	用于管理从所有利益相关者的期望、客户需求、技术产品需求到最低层次的产品部件需求的过程
风险 Risk	一个工程或项目经历非预期的事件（例如，费用超支、进度延误、轻微安全事故、健康问题、恶意行为、环境影响、未能达成所需要的科学技术突破或使命任务成功准则）的概率，以及当非预期事件发生时造成的后果、影响和严重性的组合。上述概率和后果可能含有相关的不确定性
风险评估 Risk Assessment	对项目风险的评价以确定：（1）做什么可能出现错误；（2）该错误可能如何发生；（3）该错误的后果是什么；（4）与该可能的错误和可能的后果相关的不确定性是什么
风险管理 Risk Management	一个有条理的系统的决策过程，用于有效地辨识、分析、规划、跟踪、控制、交流和记录风险，并建立缩减风险的途径和规划以提高达到工程/项目目标的可能性
基于风险信息的决策分析流程 Risk-Informed Decision Analysis Process	一个由五个步骤构成的决策过程，首先关注目标，其次关注针对了然于胸的目标开发决策方案，并且在其他系统工程流程中应用所开发的决策方案。该流程的后几步与技术风险管理流程密切相关
安全性 Safety	避免导致下列情况发生的能力和程度：死亡、受伤、职业病、设备和财产的毁坏或损失、环境破坏
搜索空间（方案空间） Search Space (or Alternative Space)	由设计约束和参数确定的概念可能性的包络，在其中可以进行方案的概念开发和权衡分析
软件 Software	与 NPD 2820.1《NASA 软件政策》中的定义相同
规范 Specification	完整、精确、可实证地规定系统或系统部件的需求、设计、行为和特征的文档
利益相关者 Stakeholder	可能受一项任务（事项）结果的影响或在某种程度上对其负有责任的团体或个人。术语“相关利益者”是“利益相关者”的子集，描述那些确认承担某项特定任务的人。利益相关者主要分为两类，参见“客户”和“其他关注团体”

续表

条 目	定义/语境
利益相关者期望 Stakeholder Expectations	未被表达为需求（未以“需要”形式陈述）的关于需要、愿望、能力和要求的阐述被看做“期望”。一旦来自利益相关者的期望被搜集、分析并转换为“需要”形式阐述，该期望变为需求。期望可以是定性的（不可度量）和定量的（可度量）。需求通常是定量的阐述。期望的形式可以是应用系统工程流程的产品功能、行为或约束的描述，也可以是对应用系统工程流程产品的描述
利益相关者期望定义流程 Stakeholder Expectations Definition Process	系统工程引擎的最初步骤，用于建立系统设计和产品实现的基础。这个流程的主要目的是辨识利益相关者，以及他们打算如何使用该产品，通过描述用例想定、设计参考使命任务和运行使用构想完成
独立评审委员会 Standing Review Board	负责针对工程/项目的每项需求进行独立评审的实体。独立评审委员会在需要特定评审时被推荐和授权，对工程/项目提交的材料进行客观评审
状态图 State Diagram	用于表示不同输入下的系统动态进展过程的图表
成功准则 Success Criteria	为令人信服地表现出技术评审目标已经实现所必须的，能够在寿命周期中取得技术进展的特定成果。成功准则根据技术评审计划归档
监督 Surveillance (or Insight or Oversight)	对承包商的进展和生产活动的监督（如状况讨论、评审、审核、场所巡视），以辨别财政责任，保证乘员安全和使命任务成功，并决定合同执行中额外的奖励费（或未达标准的罚金）
系统 System	（1）由共同作用形成满足所需要能力的单元组成。这些单元包括为实现该目的所有硬件、软件、设备、设施、人员、流程和技术规程。（2）（实现运行功能的）目标产品和（为目标产品运行使用提供寿命周期保障服务的）辅助产品组成的系统
系统验收评审 System Acceptance Review	为了验证最终系统产品有关期望成熟度水平的完整性和评估满足利益相关者期望程度进行的评审。系统验收评审检查系统、其最终系统产品和文档、试验数据，并分析他们对系统确认和验证的支持程度。它同时保证系统授权运输到指定的运行设施或发射场所技术成熟度的充分性
系统定义评审 System Definition Review	检查所提议系统结构/设计，直到系统全部功能单元所进行的评审
系统集成评审 System Integration Review	为保证系统集成已准备就绪，系统部段、部件和子系统已为集成准备就绪，保证集成设施、保障人员、集成规划和技术规程已为集成准备就绪进行的评审。系统集成评审在系统详细设计（阶段 C）结束后和系统组装、集成和试验（阶段 D）开始之前进行
系统需求评审 System Requirements Review	为检查系统的功能需求和性能需求定义，检查初步的工程或项目计划，确保需求和选定的概念满足使命任务要求而进行的评审
系统安全性工程 System Safety Engineering	在系统全寿命周期各阶段的运行效能、适用性、时间和费用约束下，应用工程和管理原理、准则和技术使系统风险达到低于可接受的轻微意外风险水平
系统结构 System Structure	系统结构由基于产品的工作分解结构模型的分层结构构成（参见工作分解结构）
系统分析 Systems Analysis	将需求转换为明确定义的可实现产品的分析过程，系统分析支持与所有物理和功能需求的兼容，支持在保证系统性能和承受能力情况下，以可靠性、维修性、保障性、耐用性、可处置性表述的运行使用想定。系统分析可以根据客户需要在寿命周期的每个阶段实施，从 A 前阶段直到目标产品的实现或更远
系统方法 Systems Approach	一种系统的、严格的工程方法，可递归、迭代、重复应用在项目或工程的寿命周期中那些集成为一个整体的系统的开发、运行和维护中

续表

条 目	定义/语境
系统工程引擎 Systems Engineering Engine	在产品寿命周期的各个阶段内规划和实施技术工作的技术流程框架。图 2.1-1 的系统工程引擎给出了产品工程研发过程中驱动技术工作的 17 个步骤
系统工程管理计划 Systems Engineering Management Plan	系统工程管理计划辨识技术工作的作用和责任接口, 以及确定如何管理这些接口。系统工程管理计划是技术途径归档和交流的载体, 包括通用技术流程的应用、资源的运用, 以及与指标体系和成功准则相关的关键技术任务、活动和事件
裁剪 (剪裁) Tailoring	对遵从特定工程或项目需求的流程和方法进行调整, 生成和审批相应的文档
技术评估流程 Technical Assessment Process	在定期技术评审中采用的辅助监测工程/项目进展的定点评估过程。它同时提供支持系统设计、产品实现和技术管理决策的相关状态信息
技术数据管理过程 Technical Data Management Process	该流程用于规划获取、评估、保护和使用反映技术本质的数据, 以支持系统的全寿命周期, 包括系统的开发、部署、运行使用和保障, 直到退役, 甚至按照 NASA 的现行政策, 在系统退役之后仍然保留相关的技术数据
技术数据资料 Technical Data Package	系统设计解决方案定义流程的输出, 随系统阶段发展而演化, 开始于概念简述和概念模型, 结束时形成完整图纸、部件清单, 以及其他在产品实施和集成中的详细要求
技术指标 Technical Measures	基于期望和需求而确立的度量指标集, 基于此跟踪和评估全系统或产品以确定其效能及客户满意度。通常这样的度量指标为效能指标、性能指标和技术性能指标
技术性能指标 Technical Performance Measures	关键性能参数集, 通过对比相关参数的当前指标与预测的当前和未来指标进行监测, 用于确定其进展或辨识其对满足系统需求可能产生危害的缺陷。所评估的参数值超出预测的期望值范围意味着需要进行评价和修正。技术性能指标通常从性能指标定义的指标集中选出
技术规划流程 Technical Planning Process	系统工程引擎包含的八个技术管理流程中的第一个, 技术规划流程建立应用和管理每个通用技术流程的计划, 这些通用技术流程用于驱动系统产品和相关工作产品的开发。该流程同时建立辨识和定义所需技术工作的规划, 以满足项目目标及费用、进度和风险约束下项目寿命周期阶段的成功准则
技术需求定义流程 Technical Requirements Definition Process	用于将利益相关者期望转换为经确认的技术需求完备集的过程, 技术需求表达为“需要”形式的陈述, 用于定义产品分解结构模型和相关辅助产品的设计方案
技术风险 Technical Risk	与技术目标、准则和目标成果相关的风险。它表现为关于技术性能、人身安全、使命任务品质和环境方面不愿看到的后果
技术风险管理流程 Technical Risk Management Process	度量和评估风险及开发管理风险策略的流程。作为探索和拓展知识的纲领, 它是管理 NASA 工程项目的重要组成部分。这个流程的关键是提前辨识对工程、项目、活动控制基线的偏离
技术团队 Technical Team	由涉及多个学科, 拥有相关领域知识、经验、资质和技能, 能完成特定技术工作的个人组成的群体
技术成熟度评估报告 Technology Readiness Assessment Report	系统从阶段 B 转入阶段 C/D 所需要的文档, 说明所有的系统、子系统和部件在相关环境中获得的验证证据支持下, 已经达到要求的技术成熟度水平
技术评估 Technology Assessment	确定需要开发新技术或将新技术引入系统的系统流程。技术评估流程在产品分解结构框架内采用系统工程的基本原理和流程, 它包含两个步骤: (1) 通过技术成熟度水平评估确定当前技术成熟度; (2) 通过采用技术改进难度评估确定将技术从一个技术成熟度水平推进到下一个技术成熟度水平的难度

续表

条 目	定义/语境
技术开发计划 Technology Development Plan	系统从阶段 A 转入阶段 B 所需要的文档,以辨识需要开发的技术、需要改进的已有系统、进行开发的备选路径、时间后端位置,以及与性能相关的阶段划分、里程碑和关键决策点。它是项目初步计划的一部分
技术成熟度评估 Technology Maturity Assessment	通过技术成熟度水平确定系统技术成熟度的过程
技术成熟度水平 Technology Readiness Level	提供度量技术成熟度依据的尺度。技术成熟度水平的范围从 1 级(基础技术研究)到 9 级(系统试验、发射和运行)。通常若将技术集成到系统工程流程中,其技术成熟度水平需要达到 6 级(相关环境中技术演示验证)
试验 Test	已实现目标产品的使用,以获得详细数据来确认系统性能,或通过进一步分析提供充足信息来验证系统性能
试验准备状态评审 Test Readiness Review	该评审保证试验品(硬件或软件)、试验设施、保障人员和试验技术规程已经准备就绪,可以进行试验及数据获取、缩减和控制
可追溯性 Traceability	在两个或多个逻辑实体(如需求、系统单元、验证、任务)之间的可辨识的联系
权衡研究 Trade Study	针对多个满足系统功能需求的系统备选设计方案进行评价的方法。该方法通过度量系统效能和费用评价备选方案,采取适当的选取原则对备选方案排序,排除前景较差的备选方案,并且在需要时,推进到系统结构下一分辨率层次实施
权衡研究报告 Trade Study Report	权衡研究形成的文档报告。其中包括被分析的系统、系统目的、系统目标(或需求,与分辨率水平相关)、系统约束、指标和度量方法(模型)、使用的全部数据源、待分析的备选方案、计算结果(包括不确定性范围和敏感性分析结果)、采用的选取规则,以及最终推荐的方案
权衡树 Trade Tree	权衡研究方案的一种表达,其中每一层代表系统需要进行权衡的某个方面,以便在权衡研究中确定最佳的系统方案
交付 Transition	将产品从其研制或集成的场所,同时也是验证和确认的场所,提交或移交给客户的行动。该行动包括包装、搬运、储存、移动、运输、安装和维护等活动
效用 Utility	从一个方案中获得相关价值的度量。效用的理论度量单位是 util
确认的需求 Validated Requirements	经过良好定义的(清晰明确)、完整的(与客户和利益相关者的需要和期望相符)、一致的(无冲突),以及可个别验证和追溯直到更高层次需求或系统目标的一组需求
确认 Validation	确保完成的产品按照需要工作所进行的试验,可能是在模拟条件下进行
(产品) 确认 Validation (of a product)	证明产品能够实现预期目的。确认可能需要通过试验、分析、演示的组合来确定
偏差 Variance	在工程控制术语中,表示实际性能与计划的费用或进度状态之间的差别
验证 Verification	证明或表明所完成的产品满足设计规范和需求的过程
(产品) 验证 Verification (of a product)	符合规范的证明。验证可能需要通过试验、分析、演示和调查的组合来确定
免责声明 Waiver	有意的不再要求计划或项目满足某项需求的文档化协议(某些 NASA 中心在实施前使用变更声明,而在实施过程中使用免责声明)

续表

条 目	定义/语境
工作分解结构模型 WBS Model	系统描述模型，包括目标产品及其（完成系统运行功能的）子系统、保障和辅助产品，以及系统开发中需要的各种其他工作产品（规划、控制基线等）
工作分解结构（WBS） Work Breakdown Structure (WBS)	根据开展工作的途径构造的，针对生产工程/项目目标产品需要的硬件、软件、服务和数据进行的面向产品的层次化分解，反映工程/项目的费用、进度、技术和风险数据采集、综合和报告的方法
工作流图 Workflow Diagram	表明活动、活动的关系和里程碑的进度示意图

附录 C 如何撰写一个好的需求

1. 术语的正确使用

- 需要 (Shall) = 反映需求
- 能够 (Will) = 反映事实上的或宣称的目的
- 应当 (Should) = 反映目标

2. 编写清单

1) 人员需求

形式为“责任方需要如此执行”的需求。换句话说，使用主动态语言，不使用被动态语言。需求必须表述为“谁需要”按照必须执行的事项描述去（做、执行、提供、赋权或其他动词）。

2) 产品需求

(1) 形式为“产品 ABC 需要 XYZ”的需求。需求必须表述为“产品需要”按照必须完成的事项描述去（做、执行、提供、权衡或其他动词）。

(2) 需求针对产品及其低层的实体使用一致的术语。

(3) 需求包括容许定性/性能值的计算（如小于、大于或等于，正值或负值，3 西格玛平方和求根）误差。

(4) 需求是否不涉及实施过程？（需求应当表述为需要的是是什么，而不是如何提供它；即表述问题而不是解决方案。询问“为什么提出这个需求？”，则答案可能指向真实的需求）。

(5) 需求是否不涉及运行使用描述？（这是一个产品必须满足的要求，还是一个包含了产品的活动？像“操作员需要执行……”这样的语句几乎就是运行陈述而非需求）。

3) 产品需求示例

- 系统运行的能量水平需要在……
- 软件获取的数据需要来自……
- 结构承受的载荷需要达到……
- 硬件的质量需要是……

3. 一般完好性准则

(1) 需求描述在语法上是正确的。

(2) 需求描述不存在键入、拼写和标点错误。

(3) 需求描述遵从项目模板和文体规则。

(4) 需求是正面表述的（而不是负面的，如表述为“不能”）。

(5) “待确定”参数值的使用应减到最少。最好是使用参数值的最佳估算，并标记为“待解算”，同时推断出为消除“待解算”参数必须做什么，谁负责消除它，以及什么时候它必须消除。

(6) 需求伴有可理解的推断，包括任何假设。你能确认（同意）这些假设吗？假设在作为研制基础前必须得到证实。

(7) 需求位于文档中的合适章节（例如，不作为附录）。

4. 需求的确认内容

1) 清晰性

(1) 需求是否清楚明晰？（需求的所有方面是否都是可理解的，并且不会出现曲解？需求中是否未出现不定代词（这、这些）及模糊语（如“大约”、“等等”、“与/或”、“但不限于”）？）

(2) 需求是否简单明了？

(3) 需求中的每条需求表述是否仅表达唯一想法？一个表述中是否仅表达单一需求而不是多个需求，或一个段落中是否不会同时包含需求和推断？

(4) 需求陈述是否仅有一个主语和一个谓语？

2) 完整性

(1) 需求表述是否尽可能完整？是否所有不完整的需求被标记为“待确定”或“待解算”，是否能够维护需求的完整列表？

(2) 是否遗漏任何需求？例如，下列需求领域中是否有任何被忽视的：功能、性能、接口、（开发、制造、试验、运输、储存、运行）环境、（制造、试验、储存、运行）设施、（制造、组装、交付、储存、装载）过程中的运输、训练、人员、操作性、安全性、保密性、外观及物理特性、设计。

(3) 所有的假设是否清晰表述？

3) 适用性

(1) 所有需求是否针对正确层次（如系统、部段、单元、子系统）？

(2) 所有需求是否不涉及实施细节（需求应当表述需要什么，而不是如何提供它）？

(3) 所有需求是否不涉及运行描述（不要混淆运行和需求：可在运行使用构想中更新）？

4) 一致性

(1) 需求描述是否一致，而不存在自相矛盾，且不存在相关系统的需求？

(2) 术语是否与用户和主管方的术语一致？是否与项目词汇表中术语的一致？

(3) 术语是否在文档中始终保持一致？

(4) 关键词汇是否包含在项目词汇表中？

5) 可追溯性

(1) 所有需求都是必须的吗？每项需求都需要满足其高层需求吗？每项需求都是必须的功能或特征吗？要区别需要的和想要的。如果不是必须，那就不是需求。询问“如果不包括此需求，可能发生的最坏结果是什么？”

(2) 是否所有需求（功能、结构和约束）双向可追溯到高层需求、使命任务或待研系统的范畴（包括需要、目的、目标、约束、运行使用构想）？

(3) 每项需求的表述方式是否能够在其他相关文档中被唯一引用（如每项需求具有唯一标号）？

6) 正确性

(1) 每项需求是否正确？

(2) 每项假设表述是否正确？假设在作为研制基础前必须得到证实。

(3) 需求在技术上是否可行？

7) 功能性

所有描述的功能是必须的吗？所有功能是否充分满足使命任务和系统目的和目标？

8) 性能

(1) 所有需要的性能规格和余量是否列出（如对时间限制、生产能力、储存空间、时间延迟、精确度等因素的考虑）？

(2) 是否每项性能需求是现实的？

(3) 误差许可是否过严？误差许可是否可推敲和经济有效？询问：“如果误差许可扩大两到三倍，可能发生的最坏结果是什么？”

9) 接口

(1) 所有外部接口是否清晰定义？

(2) 所有内部接口是否清晰定义？

(3) 所有接口是否必要、充分，相互之间是否一致？

10) 可维修性

(1) 系统可维修性需求是否以可度量、可验证的方式规定？

(2) 书写的需求是否使得变更产生的连锁反应为最小（即需求之间的耦合性尽可能弱）？

11) 可靠性

(1) 是否确定清晰定义、度量、验证的可靠性需求？

(2) 是否有错误检测、报告、控制和修复方面的需求？

(3) 是否考虑了非期望事件（如单个出错事件、数据丢失或不规则、运行错误）及需要做出的响应？

(4) 关于功能预期结果的假设是否陈述？这些结果是必需的吗？

(5) 从硬件、软件、运行、人员和技术规程的角度看，这些需求是否适当强调了当系统出现硬件或软件故障时的生存性？

12) 可验证性/可测试性

(1) 系统可否通过试验、演示、观察或分析来表明其满足需求？这些是否能够在陈述需求的系统相应层次上完成？是否存在能够度量达到需求及验证系统对需求符合度的方法？是否能够做出这种验证准则的陈述？

(2) 需求是否精确陈述，以便于制定系统成功试验准则和需求规范？

(3) 需求是否避免了不可验证词汇（如柔性的、容易的、充分的、安全的、特别的、适当的、适合的、友好的、可用的、按需的、若需的、恰当的、快速的、便携的、轻量的、微小的、最大的、最小的、健壮的、清晰的，以及其他相似词汇）？

13) 数据使用

什么时候“无关”条件确实“不必关心”？（“无关”条件标识那些条件值或标记值不相关的情况，即使这些值对其他条件可能很重要）。无关条件值是否明确陈述？（正确标识“无关”条件可以提高设计的可移植性）。

附录 D 需求验证矩阵

在开发需求时，明确验证需求的方法是重要的事情。本附录提供一个定义了如何验证所有需求的矩阵。这个矩阵中仅包括“需要”形式表述的需求。该矩阵应该用单一的标识辨别每一个“需要”形式表述的需求，并且对于需求来源（即从中取出需求的文档）是确定的。这个矩阵可以根据项目的需要分解为多个子阵来刻画需求的来源（如每个需求文件一个子阵）。表 D-1 中给出了验证矩阵应当包含的最少信息准则的建议。

表 D-1 需求验证矩阵

需求序号 ^①	项目 1	项目 <i>i</i>	系统 <i>i</i> 或其他独立标识
文档 ^②	xxx	xxx	xxxxx（其他规范、接口控制文件等）
章节 ^③	3.2.1.1 能力：支持上行链路传送数据	其他章节	其他章节
“需要”表述 ^④	系统 X 需要提供关于……的最大地面到空间站的上行链路	阶段技术评审中其他“需要”形式表述	在规范、接口控制文档等其他“需要”形式表述
验证通过准则 ^⑤	（1）系统以最大和最小容许数据率与上行链路链接； （2）系统以最大和最小容许处理频率与上行链路链接	其他准则	其他准则
验证方法 ^⑥	试验	xxx	xxx
设施或实验室 ^⑦	xxx	xxx	xxx
阶段 ^⑧	5	xxx	xxx
验收需求 ^⑨			
飞行前验收 ^⑩			
实施组织机构 ^⑪	xxx	xxx	xxx
结果 ^⑫	技术问题摘要（xxxx号）	备忘录（xxx号）	报告（xxx号）
<p>① 每个系统及其需求具有的单一标识。</p> <p>② 包含系统及其需求在内的文档编号。</p> <p>③ 系统及其需求的章节编号。</p> <p>④ 系统及其需求（合理）文本，即以“需要”形式表述。</p> <p>⑤ 系统及其需求验证通过的准则。</p> <p>⑥ 系统及其需求的验证方法（分析、观察、演示或试验）。</p> <p>⑦ 用于进行验证和确认的设施或实验室。</p> <p>⑧ 需要进行验证和确认的阶段：开发前设计验证；正式交付时功能性验证；正式交付时环境性验证；正式系统层环境性验证；正式系统层功能性验证；正式全系统功能性验证；集成飞行器功能性验证；在轨飞行功能性验证。</p> <p>⑨ 表示该需求是否在每个单元的初始验收试验中进行验证。</p> <p>⑩ 表示该需求是否在每个单元的飞行前验收试验或再次飞行验收试验中进行验证。</p> <p>⑪ 负责进行验证的组织。</p> <p>⑫ 表示包含满足需求客观凭据的文档。</p>			

附录 E 创建确认计划（包括需求确认矩阵）

在开发系统需求时，选定确认方法是非常重要的，包括如何采用额外的确认评价、试验、分析及其他演示验证，以保证客户/投资方满意。

本确认计划应当包括一个确认矩阵，其元素见表 E-1。矩阵中的最后一列使用一个显示部件作为例子。

表 E-1 需求确认矩阵

确认产品序号	确认产品的单一标识	1
活动	描述客户/投资方将进行的评价	客户/投资方将对备选显示器进行评价
目标	客户/投资方的评价实现什么目标	（1）保证清晰度可接受；（2）保证整体外观可接受
确认方法	对系统 X 需求的确认方法（分析、调查、演示或试验）	试验
设施或实验室	用于进行确认的设施或实验室	xxx
阶段	进行验证/确认的阶段 ^①	阶段 A
实施组织	负责协调确认活动的组织	xxx
结果	指明确认活动产生的客观证据	
① 示例：在产品选择过程中；在目标产品（如果是现货产品）选择或初步设计评审之前；在关键设计评审之前；针对黑箱层功能；针对系统级功能；针对产品级功能；针对集成运载器级功能；针对在轨飞行级功能。		

附录 F 功能、时序和状态分析

1. 功能流框图

功能分析可以应用多种方法，其中之一便是功能流框图。功能流框图定义系统功能并描述功能事件时序。该方法明确“什么”必须发生，而对功能“如何”实现不做专门回答。该方法面向功能，而非面向解决方案。

功能流框图由功能模块组成，分别代表一项需要完成的明确有限的离散行动。功能架构由一系列层次化的框图开发，说明功能分解并展示功能之间的逻辑次序关系。模块用统一编号方式标识。通过编号建立贯穿整个框图的标识和关系，并利于从低层到顶层的追溯。第一层（顶层）框图的每个模块可以扩展为第二层框图功能序列，以此类推（见图 F-1）。连接功能的线段表明功能流，而非时间推进或即刻活动。框图通常按流向自左向右展开。箭头通常用于指示流向。框图同时显示输入（“转移至运行轨道”）和输出（“转移到 STS 轨道”），这样有利于接口及控制流程的定义。

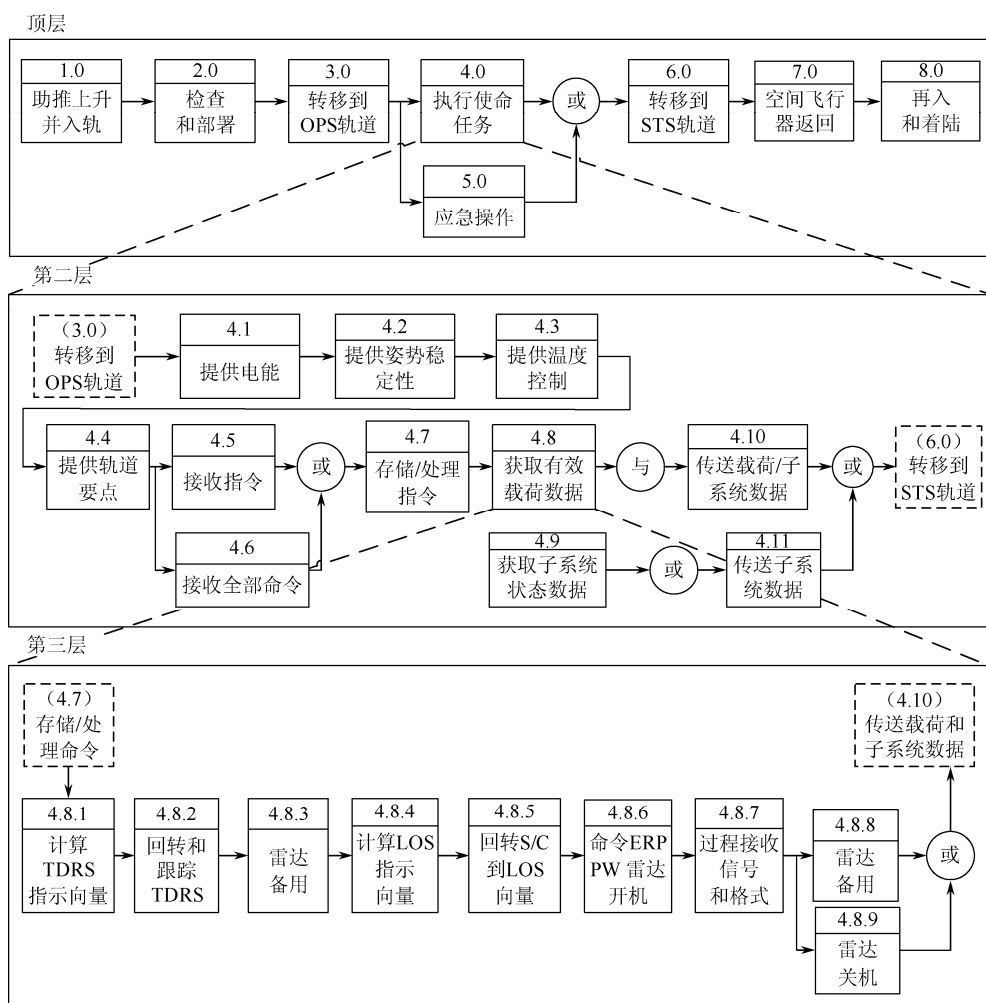


图 F-1 功能流框图分解实例

每个框图包含相对其他框图的参照，有利于在不同框图之间切换。使用逻辑门：“与”、“或”、“继续/终止”，有时为增强功能，还用到异或、迭代、重复及循环等逻辑。圆表示求和门，用于与/或门情况。与门用来呈现并行功能，所有条件都满足才能推进（即并发）。或门用来表示满足推进的路径选择。 G/\bar{G} 表示继续/终止条件。这些符号位于连线附近表示路径选择。框图示例如图 F-2 和图 F-3 所示。

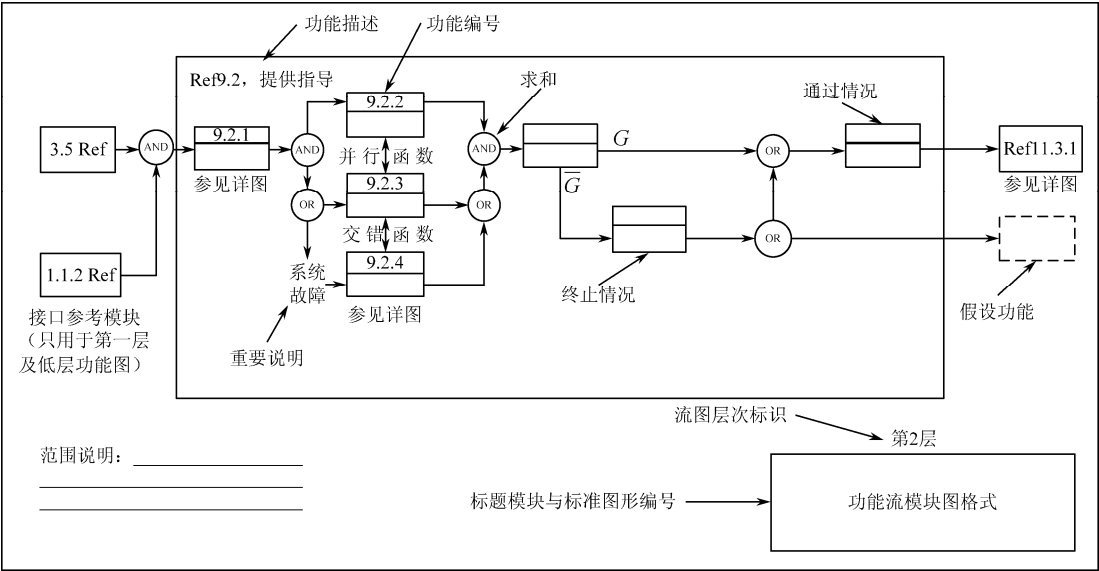


图 F-2 扩展的功能流框图：示例 1

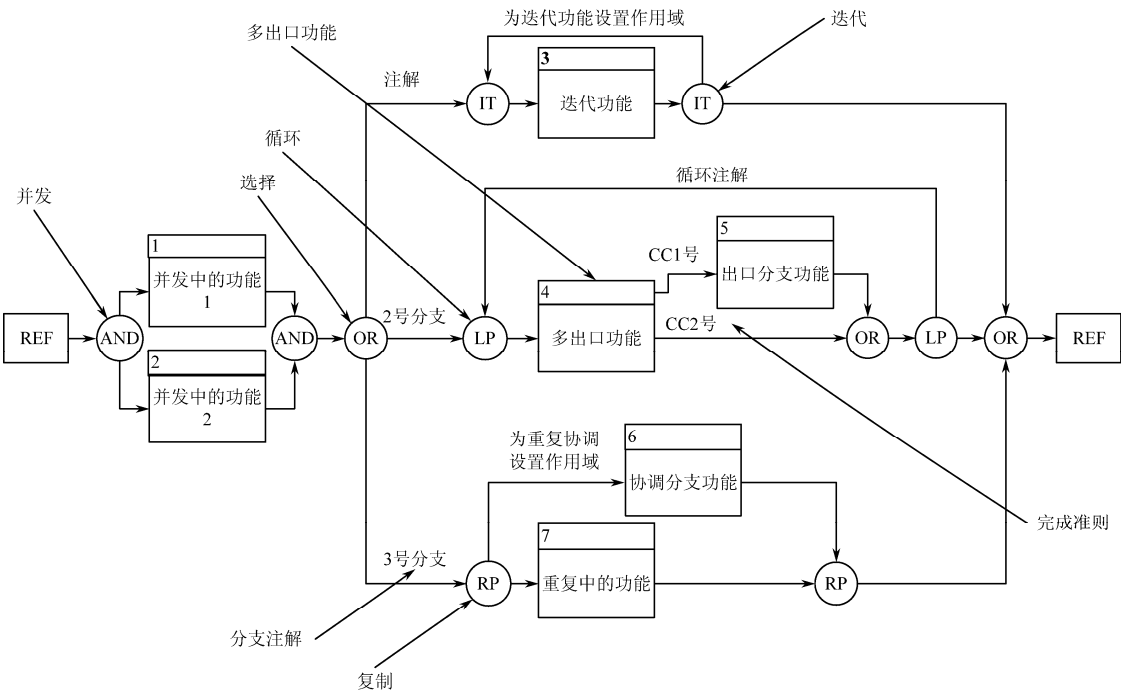


图 F-3 显示附加控制结构的功能流框图：示例 2

扩展功能流框图提供数据流覆盖以获得数据依赖关系。扩展功能流框图（见图 F-4）描述：功能；控制流；数据流。系统扩展功能流框图规范是完备的可执行离散事件模型，能够动态及静态确认。扩展功能流框图提供控制结构及数据触发两种方式指定系统功能执行条件。扩展功能流框图在图形上区别触发和非触发的数据输入。功能执行前需要触发数据。触发器实际上是有控制含义的数据项。

在图 F-4 中，触发数据输入用深色背景且两边都有箭头的数据框表示。非触发数据输入用浅色背景及单边箭头的数据框表示。扩展功能流框图必须具备：（1）在控制结构中其前方功能执行完成；（2）若有触发数据，在执行之前触发。例如，在图 F-4 中，在“3 并发功能”执行前，“1 序列功能”必须完成且“数据 3”准备就绪。应当注意输入“1 序列功能”的外部输入数据，以及来自“6 输出功能”的外部输出数据不应与此功能的单用箭头表示的功能性输入输出相混淆。数据流用圆角矩形框表示，而功能以直角矩形框来表示。

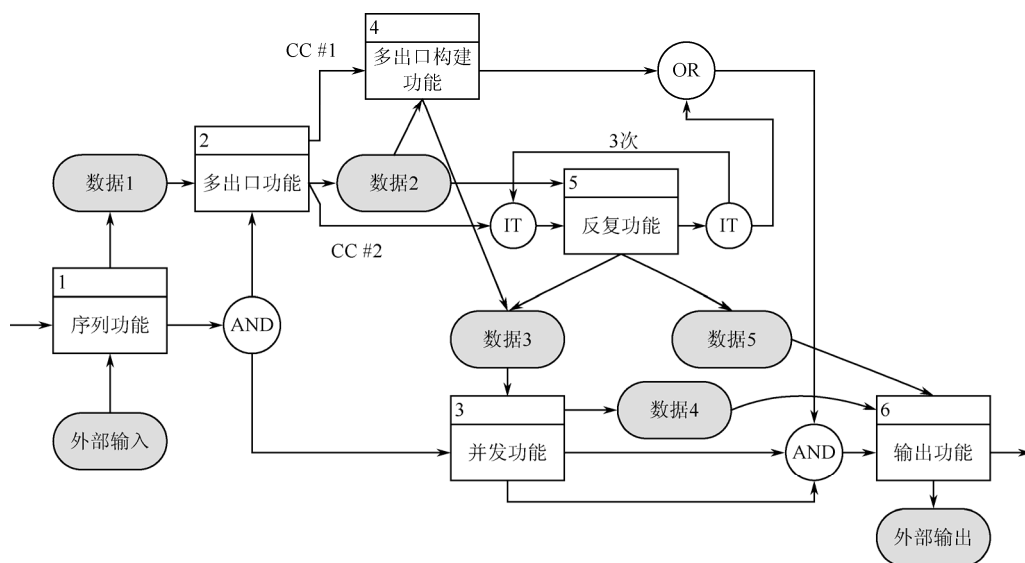


图 F-4 扩展的功能流框图：示例 3

功能分析跨越寿命周期全程。部署系统所需功能与系统运行和最终处置所需功能完全不同。寿命周期每个阶段及阶段过渡中，生成功能流框图需要绘制全部需求。这些框图用于开发需求和确定利益。功能分析还需考虑备选或应急的运行使用，以提高使命任务成功概率。功能流图提供对系统全部运行操作的理解，可作为开发系统运行和应急技术规程的基础，并确定运行技术规程中能够简化整个系统运行使用的变更内容。功能流图最终汇入工作分解结构从而决定整个使命任务的组织与成本。某些情况下，不同的功能流框图可能用于描述各种满足特定功能的方法，直到获取相关数据方选定最终的功能流框图。关于功能流框图或扩展功能流框图的更多内容可参见 Jim Long 的《系统工程中公共图形建模之间的关系》。

2. 需求分配表单

需求分配表单记录分配的功能、性能及物理系统之间的关联。表单为技术需求定义中的功能分析活动与逻辑分解及设计方案定义活动提供了可追溯关系，并维护其相关的一致性，还描述不相关性。图 F-5 所示的是需求分配清单的示例。最右边的“参考”列显示相应的功能流框图中功能序号。

ID	描 述	需 求	追 溯 自	性 能	余 量	注 释	参 考
M1	使命轨迹	57515 km太阳同步dawn-dusk 轨道	S3,S11,P3	一致	NA	加长Pegasus 与 HAPS 共同提供所需的发射剂	F.2.c
M2	运载工具	加长Pegasus 与 HAPS	P2, P4	一致	NA		F.2.c
M3	天文台质量	天文台的总质量不超过 241 kg	M1,M2	192.5kg	25.20%		F.5.b
M4	数据采集质量	完成使命需要以低于十万分之一的误码率传递95%的数据	P1	一致	NA	满足系统基线准的标准余量,应用PDR所完成的正式的系统分析	F.7
M5	通信带宽	完成任务应该使用S-band SQPSK,且从太空船下载数据不低于5Mbps,上传不低于2Mbps	S12,P4	一致	NA	见 SC27, SC28, 及G1, G2	F.3.f, F.7
M7	跟踪	在用天文台进行跟踪时主操作控制器应该使用NOKAD的两线 (two-line) 元素	P4	一致	NA	满足系统基线准的标准余量,应用PDR所完成的正式的系统分析	F.7
M8	数据潜伏期	数据潜伏期应少于 72h	P12	一致	NA		F.7
M9	每日数据量	每日提供原始科学数据量的均值应该在0.8G比特左右	P1,S12	一致	12%	具体余量的确定要根据地面指令	F.3.e, F.7
M10	地面站	本任务中的地面站应与Rutherford Appleton Laboratory地面站和Poker Flat 地面站一致	P1	一致	NA		F.7
M11	轨道残片 (伤亡区域)	如果有另一个相同轨道的天文台进入现在轨道,遭到毁伤的概率小于万分之一	S12,P4	P31/51000	400%	见附录-7的“轨道残片分析”	F.2.e, App.6
M12	轨道残片 (生命周期)	此任务结束后,再入轨的天文台小于25年	P3	小于10年	15年	见附录-7的“轨道残片分析”	F.2.e, App.6

图 F-5 需求分配表单

完成需求分配清单需要执行以下几步:

- (1) 包含功能流框图中的功能及功能序号。
- (2) 将功能上的性能需求与设计需求分配给适当的功能 (多项需求分配到单项功能,或单项需求分配给多项功能)。
- (3) 所有系统级的需求必须分配到一项功能以确保系统满足所有系统需求 (没有分配到需求的功能应作为不需要的活动剔除)。
- (4) 分配所有派生需求到相应产生需求的功能。
- (5) 确定为满足需求所用到的物理装置、技术状态、物品、设施及规范 (需求分配表单的参考内容,见美国国防部的《系统工程基础指南》)。

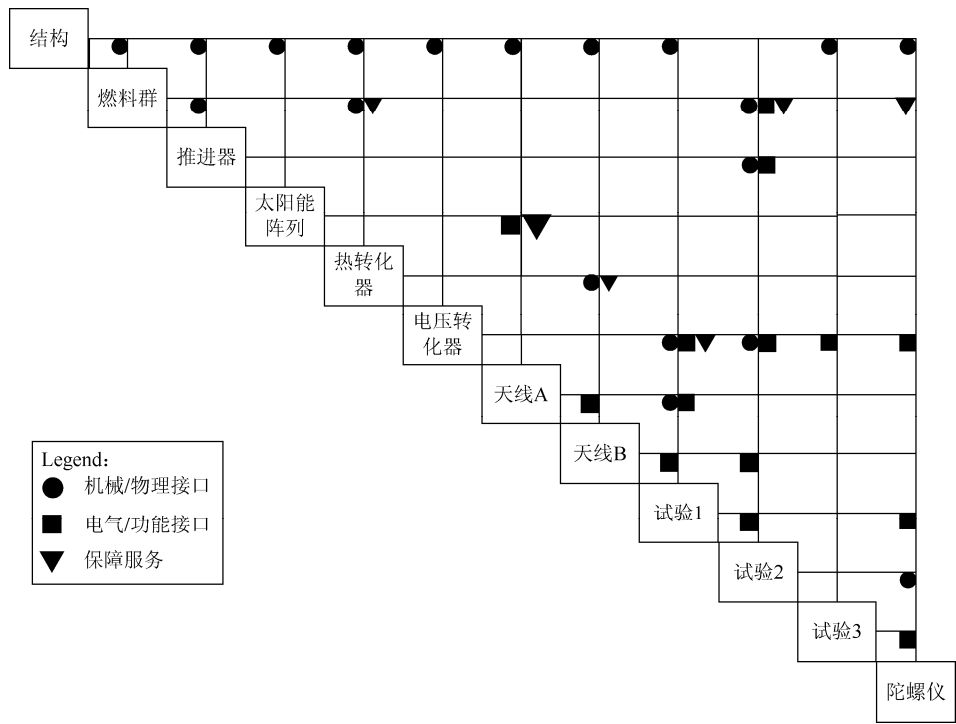
3. N2 图

N 平方 (N2) 图是特定层次结构上表示系统单元之间的功能接口和/或物理接口的矩阵。在软件领域, N2 图被广泛地应用于开发数据接口。其实, N2 图也可用于开发硬件接口, 如图 F-6 所示。系统组件放置在对角线上。NxN 方阵的剩余区域代表接口。N2 方阵中行与列的交叉点包含了相应行与列的组件之间的接口描述。例如, 太阳能电池阵列与结构之间有物理接口, 与电转换器之间有电气接口和保障服务接口 (原文如此, 与图中所示不符)。空白处代表相应组件之间没有任何接口。

N2 图可以连续地分解为更低层次上的硬件与软件组件之间的接口关系。除了定义必须通过接口提供的数据, N2 图还可以通过显示数据流确定可能在接口中引发的冲突之处, 突出表现输入与输出的依赖假设与需求。

4. 时序分析

有多种方法可以将系统中复杂的时序关系可视化。两种比较重要的方法是时序图与状态转移图。时序图 (见图 F-7) 在时间轴上定义不同对象的行为。时序图为对象的状态改变和随时间交互提供图形化描述。时序图可用于定义硬件驱动和/或软件驱动的组件行为。尽管简单的时间线分析对理解并发、覆盖、顺序关系很有用, 而状态图 (见图 F-8) 更具灵活性, 可以描述循环、决策等时间线上变化较大的事件。时序信息可加入功能流框图进行时间线分析。这在分配资源及生成特定的时间相关设计需求时十分有用。它同时阐明性能特征及设计约束, 然而它并不完整。状态图需要显示系统在输入变化情况下的反应。



注：来自 NASA 参考出版物 1370 《接口单元定义和训练手册》。

图 F-6 轨道设备的 N2 图

时序分析工具相当简单。有现成的商业产品可以使用，任何图形工具和好的电子表格软件即可完成。重要的是记住时间线分析适合分析线性流，而状态图可更好地描述循环、回路、多路径及其组合的情况。复杂性应保持分层并反映在功能流框图中。应用这些技术的最终目标是使系统思考过程足够详细，以尽可能避免出现大的意外。

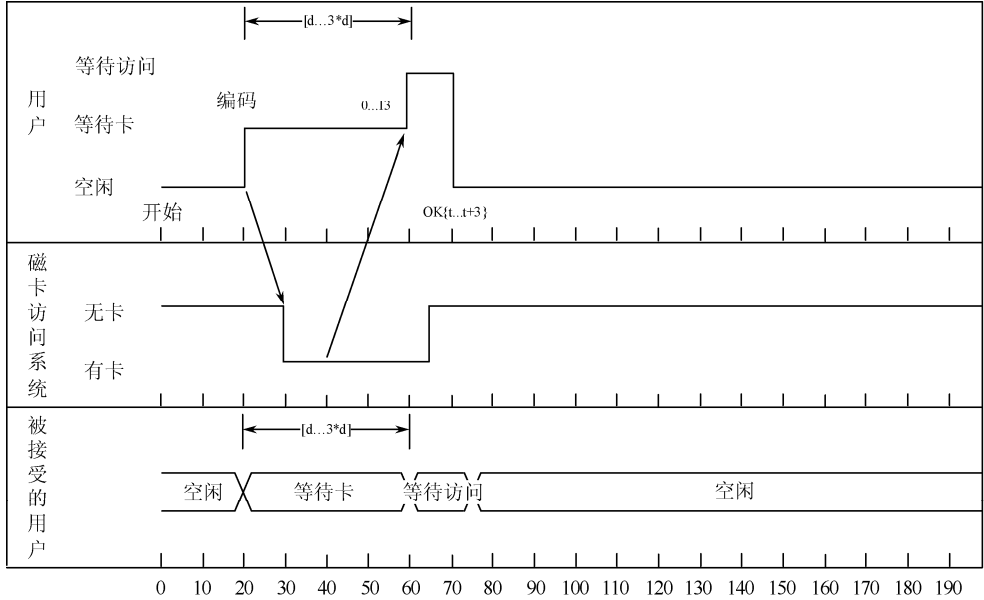
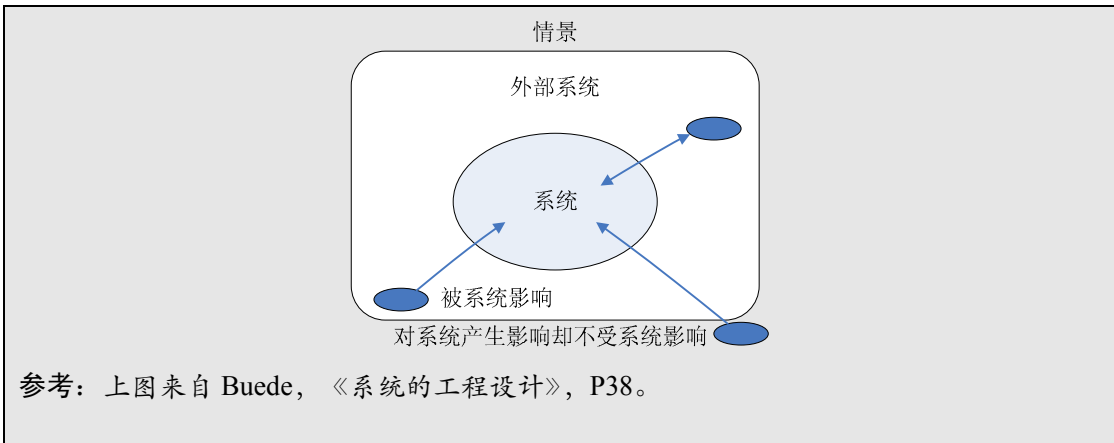


图 F-7 时序图示例



附录 G 技术评估/技术引入

1. 引言、目的和范围

NASA 的工程和项目，由于其自然属性，经常需要开发与注入新的技术进展以满足任务目标、目的和特定需求。某些情况下，新技术引入就是传统系统在原有的设计基础上，采用不同的体系结构并在不同的环境下工作。在后一种情况中，通常可能认为传统系统的改造并不需要技术进步，因而导致对开发流程中的关键步骤关注不足，从而对工程/项目造成损害。在（新的与传统改造）两种技术革新中，技术引入是个复杂的过程，多年以来，许多项目都采用不同的特定方式进行技术引入，而成功程度也不尽相同。

通常技术引入会导致进度延误、成本超支，偶尔甚至使项目取消或失败。事后检验表明，这些事件的根本原因常被归结为“需求定义不够充分”。如果失败根源确实如此，则纠正这种状况就简化为需要更好地定义需求的问题，但是看起来历史不断地重复，表明并非上述原因——至少不全部是。

实际上，导致进度延迟、成本超支和项目取消或失败的因素有很多，需求定义不充分只是其中之一。情况可能是多数因素与项目开始时的不确定性程度相关，且不确定性的主导因素是对取得项目成果所需的技术成熟度缺乏理解，随之对将技术成熟度从目前状态推进到能够通过验证并高置信水平成功引入的状态所需成本与进度余量缺乏理解。尽管这种不确定性难以消除，但通过尽早将系统工程实践应用到对技术需求的理解、对所需技术成熟度的理解，以及满足工程/项目目的、目标和需求的理解，可以充分缩减这种不确定性。

可以应用大量的流程开发成功技术引入所需的适当层次的理解。本附录的目的是描述可作为示例的系统化流程，确定如何应用系统工程实践开展综合的技术评估。技术评估由两部分组成，即技术成熟度评估及技术改进复杂度评估。流程从技术成熟度评估开始，以 NASA 的技术成熟度水平为标度确定技术成熟度。随后应用技术改进复杂度评估开发对提高技术成熟度需要什么的理解。需要在工程/项目的各个阶段进行技术评估，以获得阶段过渡所需要的关键决策点产品（参见表 G-1）。

表 G-1 技术评估为工程/项目阶段提供的产品

控 制 门	产 品
关键决策点 A——从 A 前阶段到阶段 A 的过渡	需要进行潜在技术需求与计划技术成熟度和当前技术成熟度之间的对比评估，以及对使用商业、学术及其他政府部门技术资源的机会的评估。作为集成控制基线草案的一部分
关键决策点 B——从阶段 A 到阶段 B 的过渡	需要技术开发计划，确定需要开发的技术、需要修改的传统系统、工作开展的可选途径、性能未达标及相应回退位置、里程碑、指标体系及关键决策节点。作为初步项目计划的一部分
关键决策点 C——从阶段 B 到阶段 C/D 的过渡	需要技术成熟度报告说明所有系统、子系统及组件达到的技术成熟度水平，给出在相关环境中合格应用的证据

初始技术成熟度评估提供工程/项目开始阶段系统所需技术的基准成熟度，并允许在开发

全过程监控技术进展。在初步设计评审之前开展最终的技术成熟度评估。它是技术成熟度评估报告的基础，记录通过试验与分析得到的系统、子系统、组件所需技术进步的成熟度。初始技术改进复杂度评估提供开发初步成本与进度计划和初步风险评估所需的材料。后续评估中，相应信息可在确定可选路径、回退位置和性能是否达标的过程中，构建技术开发计划。这些信息在为后续挣值管理准备里程碑和指标体系时十分关键。

技术成熟度评估需按照工程/项目的产品分解结构中硬件及软件产品的层次分解开展，以达到对系统、子系统、组件层次的系统化全面理解（见图 G-1）。

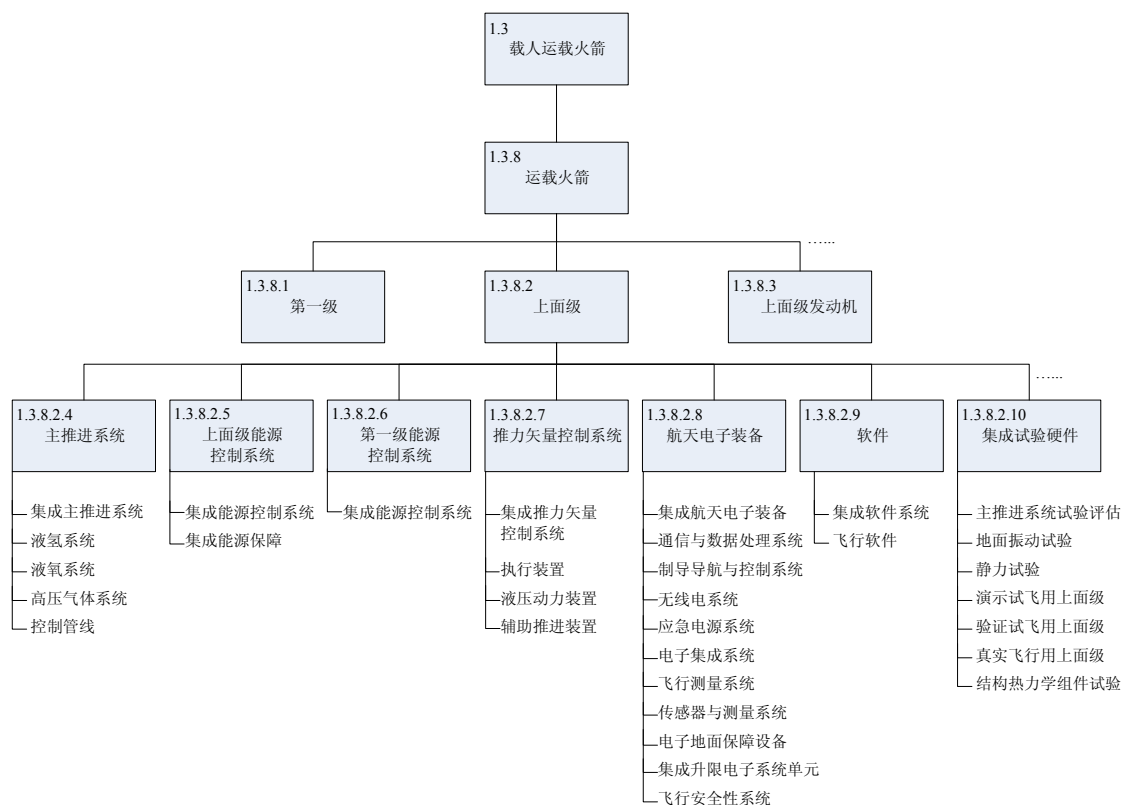


图 G-1 产品分解结构示例

2. 输入/启动准则

在工程/项目初始阶段定义技术评估流程并在整个工程/项目中通过尽早阶段的初步设计评审（概念开发）实施技术评估是极其重要的。根据工程项目的各阶段，技术评估流程的输入有不同的详细程度，甚或在 A 前阶段细节不足时，技术评估可以得出所需的主要关键技术进步。因此，在 A 前阶段开始时，应该提供以下内容：

- 技术成熟度水平定义的细化。
- 技术改进复杂度的定义。
- 用于评估流程的术语定义。
- 建立有意义的评价准则和指标体系，有利于明确性能的差距与不足。
- 成立技术评估团队。
- 独立的技术评估评审团队的成立。

术成熟过程是必须做到的。类似地，向技术开发流程提供有关需求变更的反馈，对于架构研究是必须做到的。必须给予“传统”系统格外关注，尤其是当其应用的架构与环境不同于其设计的运行使用的架构与环境时。

4. 确定技术成熟度水平（TRL）

技术成熟度水平最基本的含义是描述给定系统、子系统、组件的性能历史，1980 年在 NASA 总部首次使用。技术成熟度水平主要描述给定技术的当前水平并提供计量技术成熟度及技术进步的控制基线（见图 G-4）。尽管技术成熟度水平概念已经提出了近 30 年，但并没有被熟知反而经常被曲解。其结果是，既不明确所承担工程的关键技术成熟度，也不清楚为开发所需水准的技术应当做什么。如果对于系统所有单元的基准技术成熟度没有清晰的把握，就不可能了解工程的重要性与开发范围。确定技术成熟度水平是工程成功至关重要的第一步。常见错误观念认为在实践中很难确定技术成熟度水平，并且这样做没有意义。相反，确定技术成熟度水平是直接的系统工程流程，只需确定证明什么和在什么条件下证明。

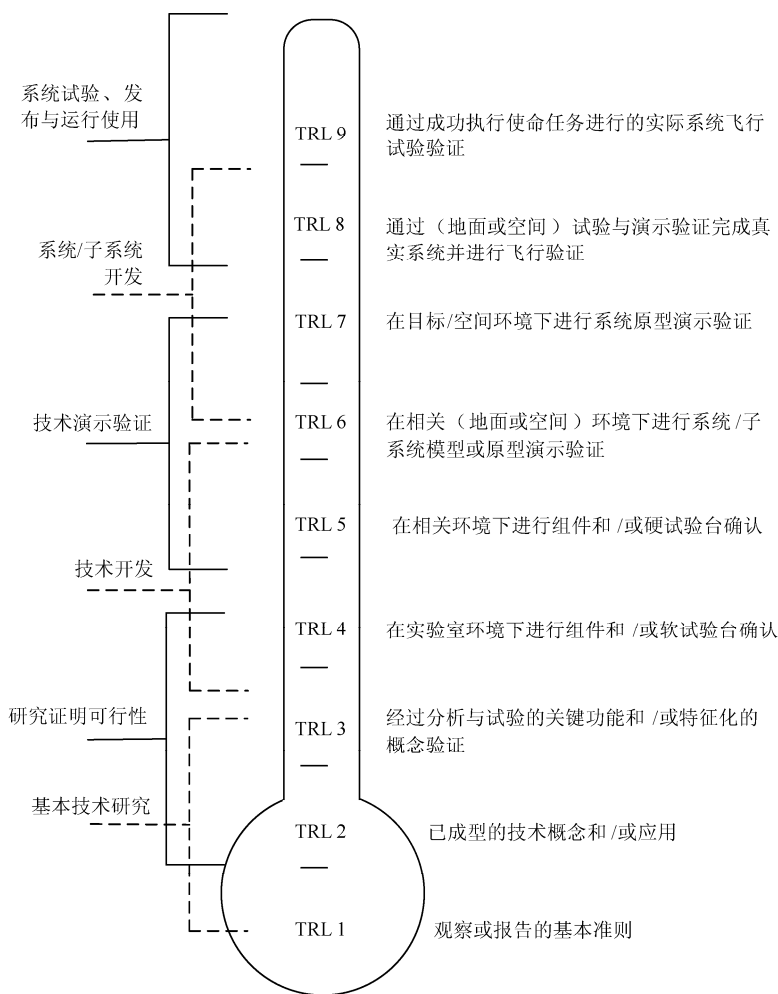


图 G-4 技术成熟度水平

一眼看去，图 G-4 中描述的技术成熟度水平显得很直接。问题出现在试图将其分配到各

层时。困难的主要原因是术语，人人都知道“试验台”是什么，但是定义却不同。同样，什么是“相关环境”？与某个应用相关却可能与其他不相关。许多术语来源于不同的工程背景，在特定领域有特定含义。它们最终在工程领域广泛应用，但在不同学科有不同含义，其差异可能很小，也可能很大。例如“试验台”，来源于电子工程领域，其本意是指利用元器件组装成试验板检验电路的功能设计，以验证设计是否与预期一致。其他来自于机械工程领域的术语，是指试验中承受不同级别压力的元件，即合格试验、试飞试验和飞行元件。开发统一的技术成熟度水平评估（见图 G-5），第一步定义所用术语。在工程/项目活动中，开发并使用一致的定义集合至关重要。

建立起通用术语集后，需在以往经验的基础上，推进到下一步——量化判断准则。即使有清晰的定义，在评估给定元件与所需元件的相近程度时仍需要有判断准则（即原型是否与期望的原型相近，或它仅像是工程试验台？）。以外形、匹配和功能的形式描述已完成工作，为检验单元是否符合设计意图及相应性能提供了手段。软件技术成熟度水平的定义包含在 NPR 7120.8《NASA 研究与技术工程和项目管理需求》中。

评估的第三个关键因素与回答谁最适合针对有问题的技术状况确定判断准则这个问题相关。在这一步，拥有均衡的经验丰富的评价团队极端重要。团队成员不必是学科专家。技术成熟度水平评估所需的专业知识主要是系统工程师/用户对当前应用状况的理解。建立了定义集，定义了量化判断准则流程，并组成了专家评价团队后，主要流程就是提出正确问题。图 G-5 所示的流程图呈现了评估中在任何层级上确定技术成熟度水平所需要提出的问题。

注意第二个框特别针对传统系统。如果架构和环境发生变化，则技术成熟度水平降到 TRL5，至少开始如此。针对新应用和新环境需要对传统系统进行附加试验。如果后续分析中新环境充分接近旧环境，或新架构充分接近旧架构，则相应评价可以为 TRL6 或 TRL7，而重要的是了解此时不会再有 TRL9。首先在系统层应用该流程，继而应用到更低层的子系统和组件，如此确定需要开发的单元并设定后续阶段，最后确定技术改进复杂度。

形成该流程的方法如图 G-6 所示。这里，流程以表格形式呈现：每“行”列出需要评价的系统、子系统、组件。“列”代表用于确定技术成熟度水平的种类，即已构建哪些元件，到何种程度，在什么环境中进行过试验。对这些问题的回答将确定所考虑产品的技术成熟度水平。系统技术成熟度水平决定于系统中最低的技术成熟度水平，即如果系统的每个单元处于 TRL2，则系统处于 TRL2。多个单元处于低技术成熟度水平的问题在技术改进复杂度流程中解决。注意每个系统、子系统、组件的集成影响。所有单元可处于较高技术成熟度水平，但若未集成为整件，则整件的技术成熟度水平更低。程度取决于集成的复杂性。

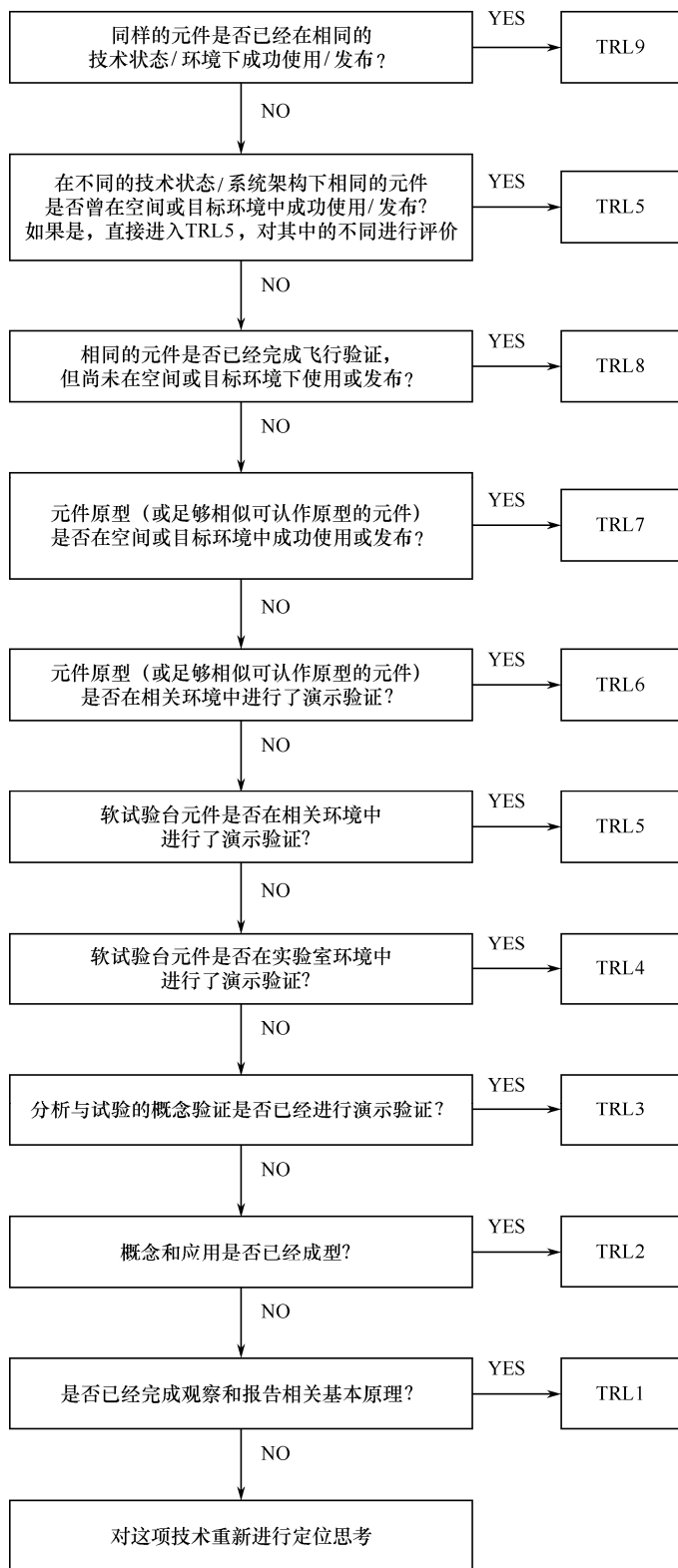


图 G-5 技术成熟度评估的思考过程

TRL评估															
		规划论证单元				环境			单元描述				总体技术成熟度		
		概念	试验板	线路板	开发模型	飞行验证	实验室环境	相关环境	空间环境	运行使用环境	形式	匹配度		功能	适用尺度
R	红色=TRL3级以下														
Y	黄色=TRL3、4、5级														
G	绿色=TRL6级（含）以上														
	白色=未知														
X	存在														
1.0 系统															
1.1 子系统X														R	
1.1.1 机械组件															
1.1.2 机械系统															
1.1.3 电子组件						X			X		X	X	X	G	
1.1.4 电子系统															
1.1.5 控制系统															
1.1.6 热力学系统							X				X	X		Y	
1.1.7 流体系统			X											R	
1.1.8 光学系统															
1.1.9 光电系统															
1.1.10 软件系统															
1.1.11 机理			X											R	
1.1.12 集成															
1.2 子系统Y														Y	
1.2.1 机械组件															

图 G-6 技术成熟度水平评估矩阵

附录 H 集成计划概要

1. 目的

集成计划定义项目中在系统设计及设计分解到较低层次单元时的项目接口集成与验证策略^①。集成计划在结构上将各个单元组装成相应子系统，并将所有的子系统合并组装为系统/产品。集成计划的主要目的是（1）描述支持设计实施策略的协同集成工作；（2）为参与者描述在集成工作的每个步骤中需要完成的工作；（3）确定所需的资源及其使用时机与使用场合。

2. 问题/清单

- 集成计划是否包含和覆盖项目中（不论自主开发还是购买的）所有组件与子系统的集成？
- 集成计划是否考虑到需要与系统集成的所有外部系统（例如，通信网络、场站设施及其他由政府或政府部门所拥有的完整系统）？
- 集成计划是否完全支持系统实施策略，例如，子系统和系统在何时何地使用？
- 集成计划是否与验证计划吻合？
- 对于集成的每一步骤，集成计划是否已定义需要集成的组件或子系统？
- 对于集成的每一步骤，集成计划是否已确定所有需要的参与者并定义他们的角色和职责？
- 集成计划是否安排所有集成步骤的顺序与进度？
- 集成计划是否阐明集成中出现的问题如何归档与解决？

3. 集成计划内容

表 H-1 分章节列出集成计划的内容。

表 H-1 集成计划内容

章 节	内 容
标题页	标题页应该遵循 NASA 的技术规程和行文指南。至少，应该包括以下内容： <ul style="list-style-type: none">• [项目名称]和[组织名称]的集成计划；• 合同号；• 文档正式批准的日期；• 负责准备文档的组织；• 内部文档控制编号（如果有）；• 修订的版本号及发表日期
1.0 文档的目的	对文档目的的简要陈述。如这这是在验证之前对项目组件和子系统的集成计划
2.0 项目的范围	本节给出已经计划好的项目及待建系统的简要描述。重点是要给出项目部署的复杂性及挑战性

^① 本附录的材料采自联邦高速公路管理局和 CalTrans 的《ITS 系统工程指导书》，2.0 版。

续表

章 节	内 容
3.0 集成策略	<p>本节告知读者集成任务的高层计划是什么，更重要的是告知集成计划为什么采用本计划中给出的结构。集成计划需服从若干相互冲突的约束。同时集成计划是更大的制造、集成、验证和部署流程的一部分，所有这些必须同步支持同一个项目策略。因此，即使对相当复杂的项目，基于清晰简明的项目目的和目标陈述，这里描述的应是高层且包含一切的集成策略。还有必要描述备选集成策略的分析，以说明为什么选择当前特定的策略。</p> <p>同一策略是构建计划、验证计划及部署计划的基础。本节覆盖并描述集成流程中的每一步。它描述每一步中参与集成的组件，给出通过集成覆盖相应运行使用能力（需求）的总体思路。它将计划与前期的目标连接起来，使得利益相关者可以理解每个集成步骤的依据。这个概要层次的描述还定义集成工作的进度安排</p>
4.0 第一阶段集成	<p>本节及后续各节，定义并解释集成流程中的每个步骤。这样做的目的是确定所有需要参与的人员并向他们描述其必须完成的工作。</p> <p>一般而言，每一集成步骤的描述应该包含以下内容：</p> <ul style="list-style-type: none">● 活动执行的场所。● 需集成的项目中开发的设备和软件产品。起初这仅是一份高层清单，而最终这份清单会精确完整地给出部件的数量和质量。● 在集成步骤中任何需要的辅助设备（模拟尚未集成的软件组件的特殊软件、试验硬件、软件、驱动程序、外部系统）。相同的辅助设备在其后的验证过程中也极有可能用到。● 所有在安装后需要开展的集成活动，包括与安装场所的系统及其他地点的外部系统之间的集成。● 对在当前集成步骤之后发生的并在相应验证计划中定义的验证活动的描述。● 集成步骤中，每个活动的负责单位。● 所有活动的进度安排
5.0 多阶段集成步骤	<p>本节及可能的附加小节，与 4.0 节的格式保持一致。每一节对应于多步骤集成工作的一个步骤</p>

附录 I 验证和确认范例概要

1. 引言

- 1.1 目的和范围
- 1.2 职责和变更权限
- 1.3 定义

2. 适用和参考文档

- 2.1 适用文档
- 2.2 参考文档
- 2.3 优先级

3. 系统 X 描述

- 3.1 系统 X 需求分解
- 3.2 系统 X 架构
- 3.3 目标产品架构
 - 3.3.1 系统 X 目标产品 A
 - ⋮
 - 3.3.n 系统 X 目标产品 n
- 3.4 系统 X 地面保障设备
- 3.5 其他架构描述

4. 验证和确认过程

- 4.1 验证和确认管理职责
- 4.2 验证方法
 - 4.2.1 分析
 - 4.2.2 检查
 - 4.2.3 演示
 - 4.2.4 试验
 - 4.2.4.1 合格性试验
 - 4.2.4.2 其他试验
- 4.3 确认方法
- 4.4 认证流程
- 4.5 验收试验

5. 验证和确认实施

- 5.1 系统 X 设计、验证和确认流程
- 5.2 试验件
- 5.3 保障设备
- 5.4 设施

6. 系统 X 目标产品验证和确认

- 6.1 目标产品 A
 - 6.1.1 开发/工程单位评价
 - 6.1.2 验证活动

- 6.1.2.1 验证试验
 - 6.1.2.1.1 合格性试验
 - 6.1.2.1.2 其他试验
- 6.1.2.2 验证分析
 - 6.1.2.2.1 热力学分析
 - 6.1.2.2.2 应力分析
 - 6.1.2.2.3 断裂控制分析
 - 6.1.2.2.4 材料分析
 - 6.1.2.2.5 电子电气部件分析
- 6.1.2.3 验证检查
- 6.1.2.4 验证演示
- 6.1.3 确认活动
- 6.1.4 验收试验
- ⋮

6.n 目标产品 n

7. 系统 X 验证与确认

- 7.1 目标产品集成
 - 7.1.1 开发/工程单位评价
 - 7.1.2 验证活动
 - 7.1.2.1 验证试验
 - 7.1.2.2 验证分析
 - 7.1.2.3 验证检查
 - 7.1.2.4 验证演示
 - 7.1.3 确认活动
- 7.2 全系统集成
 - 7.2.1 开发/工程单位评价
 - 7.2.2 验证活动
 - 7.2.2.1 验证试验
 - 7.2.2.2 验证分析
 - 7.2.2.3 验证检查
 - 7.2.2.4 验证演示
 - 7.2.3 确认活动

8. 系统 X 工程验证与确认

- 8.1 运载工具集成
- 8.2 全系统集成
- 8.3 在轨验证与确认活动

9. 系统 X 认证产品

附录 A 缩略语

附录 B 词汇定义

附录 C 需求验证矩阵

附录 D 系统 X 确认矩阵

附录 J 系统工程管理计划内容概要

1. 系统工程管理计划内容

系统工程管理计划是在项目实施中进行技术与工程活动的基础文档。系统工程管理计划在项目计划的框架下，向所有相关人员提供项目技术集成方法与活动的信息。系统工程管理计划提供特定的技术与管理信息，以帮助理解技术集成及接口，因此，其归档和审批可以看做项目在指导项目技术工作如何进行方面达成一致。在整个工程/项目计划的指导下，技术团队开发并根据需要更新系统工程管理计划。技术团队需要与项目负责人协同工作，评审系统工程管理计划的内容并取得一致。系统工程管理计划包括以下三个主要部分：

(1) 技术规划计划与控制，用于描述工程技术工作的计划与控制流程，支持系统设计、开发、试验和评价。

(2) 系统工程流程，包括针对 NPR 文件中描述的系统工程所做的特定裁剪，以及所使用的实施技术规程、权衡方法、工具及模型。

(3) 工程技术专业集成，描述多学科技术工作如何集成到系统工程流程中，并总结每个学科技术工作及在特定的相关计划中的交叉引用。

2. 目的与范围

本节提供关于系统工程管理计划的目的、范围与内容的简要描述。范围包括为生成满足相关产品寿命周期阶段成功准则的工作产品所需的系统工程技术工作。系统工程管理计划是技术团队针对给定的系统工作分解结构模型开展项目技术工作的计划，有助于满足寿命周期阶段的成功准则。

3. 适用文档

系统工程管理计划中本节列出适用于特定项目及其系统工程管理计划实施的文档，并描述特定项目技术工作应当遵循的主要标准和技术规程。执行专门的标准化任务应适当融入到系统工程管理计划的有关部分中。

本节提供项目所需使用的工程技术标准与技术规程。特定技术规程的示例可能包括所有危险材料的处置、控制室操作人员培训、特殊仪器度量技术、运输工具的特别接口文档、项目特定的维护技术规程。

4. 技术概要

本节包含描述项目技术工作需要解决的问题，以及描述与项目相关接口系统开发和集成的工作分解结构模型的目的、背景及产品的概要说明。

5. 系统描述

本节包括所要开发系统的目的/使命任务/目标的定义，系统工程管理计划中应用的系统工作分解结构模型产品目的的简要描述，以及系统预设的想定。每个工作分解结构模型包括系统目标产品及其子系统和保障/辅助产品，以及系统开发所需的其他工作产品（如计划、控制基线）。描述内容应当包括所有用做接口的系统和系统产品（包括人），以及与之相应工作分解结构模型产品如何进行物理、功能及电子形成的交互。

确定并记录系统约束，包括成本、进度和技术（如环境、设计）约束。

6. 系统结构

本节包括对工作分解结构模型如何开发、所开发的系统工作分解结构模型如何集成到项目工作分解结构中、整体系统结构如何开发的说明。本节还包括描述系统结构中产品规范树关系与图形树关系，说明系统目标产品及其寿命周期辅助产品之间的关系和接口如何在所计划的技术工作中进行管理。

1) 产品集成

本小节包括说明产品如何集成，以及在地理上分布组织和跨中心管理时，如何清晰描述产品的组织责任和相互依赖关系。这包括确定具体的组织（NASA 内部和外部的组织、其他政府部门、合同承包商或其他合作伙伴）并描述他们的角色与责任。

当系统组件或元件可用于集成时，需要清晰了解并确定进度表，建立关键进度安排事项。

2) 计划背景

本小节包含相关产品寿命周期模型的约束（如 NPR 7120.5），这些约束影响到开展技术工作应用的通用技术流程的计划与实施。这些约束提供技术工作与系统工程管理计划确定的相关产品寿命周期阶段之间的联系，相应地包括里程碑决策控制门、主要技术评审、影响项目完成的关键中间事件、寿命周期阶段、事件启动准则和成功准则、主要控制基线和其他需交付到技术工作承担者和客户的工作产品。

3) 技术工作的边界

本小节包含描述技术工作需解决的一般问题的边界。具体来讲，包括确定技术团队（在边界之内）可以控制什么，技术工作会产生什么或受到什么（在边界之外）技术团队不能控制的影响。应当特别关注的是沿着边界分布的物理的、功能的、电子的接口。

定义所要表述的系统。系统边界的描述可以包括以下内容：涉及系统目的实现的内部和外部单元/成品定义，形式上空间、时间、物理、操作的系统边界定义。另外，确定何时系统交付到运行使用状态及何时系统退役处置是非常重要的。

适当时应当包括在内的其他事项如下：

- 子系统的整体及功能性描述；
- 归档当前已建立的子系统性能特征；
- 确定并归档当前的接口及其特征；
- 开发功能接口描述及功能流图；
- 确定关键性能接口特征；
- 确定当前的集成策略及架构。

4) 交叉引用

本小节包含相应的非技术计划与关键参考材料的交叉引用，供技术工作使用。它描述在其他计划中的技术活动，作为当前技术工作的完整集成部分是如何完成的。

7. 技术工作集成

本节包含描述技术工作的各种输入如何集成到满足成本、进度和性能目标的协同工作中。

本节应当描述在系统工程流程的每个流程迭代过程中，专业工程技术学科的集成和协调。在各专业技术工作之间可能存在交叉，系统工程管理计划应当定义各专业技术的相关责任与权利。根据需要，本节应包含以下项目方法：

- 并行工程。
- 专业工程技术活动。
- 专业学科的参与。
- 专业学科的融合。
- 专业学科的作用与责任。
- 在系统分解与定义中专业学科的参与。
- 在验证与确认中专业学科的作用。
- 可靠性。
- 维修性。
- 质量保证。
- 综合后勤保障。
- 人因工程。
- 安全性。
- 可生产性。
- 生存能力/脆弱性。
- 遵从国家环境政策法案。
- 批准发射/飞行准备状态。

提供不同技术学科协调和开发任务集成的方法。例如，这可能包括集成团队方法的应用。要确保专业工程技术学科在所有技术团队和项目全寿命周期各个阶段得到适当的体现。应定义专业工程技术任务的范围与时间。

1) 责任与权利

本小节包括描述分配到相应技术工作的技术团队组织结构，并描述团队的人员如何构成及管理，包括（1）什么组织/专业组被指定为对项目具有控制权限，从而拥有对系统工程管理计划的最终签署权；（2）多学科的团队协作如何完成；（3）对每个计划的通用技术流程活动确定与定义所需的作用、责任和权利；（4）计划的团队成员的学科和专业知识水平及占用的人力资源；（5）所需的技术人员培训；（6）为项目的利益相关者或技术团队分配相应的角色、责任和权利，确保计划活动的完成。

提供组织结构图，标明每项活动具体负责的团队成员。标示权力和责任区段。定义制定决策/决策流程的权限。显示工程师/工程学科的关联性。

对下列人员和单位的系统工程角色及责任需要表述：项目办公室、用户、合同办公室技术代表、系统工程师、设计工程师、专业工程技术人员和合同承包商。

2) 承包商集成

本小节包含描述内部和外部承包商的技术活动如何与 NASA 技术团队的技术工作集成。具体包括建立技术协议、根据协议监督承包商进展、处理技术工作及产品需求变更请求、验收交付产品。本小节还需特别描述 NASA 技术团队与承包商之间的接口如何在 17 个通用技术流程中实现。例如，本小节描述 NASA 技术团队如何参与对承包商提交的设计解决方案定义文档进行评审和控制，或描述技术团队如何参与产品验证与产品确认活动。

承包商完成的系统所需关键交付产品和承包商需要向其他项目参与者提供的关键交付产品应该在进度计划中识别和确定。

3) 保障集成

本小节包含描述用于保障技术工作集成的方法（例如，集成计算机辅助工具集、集成工作产品数据库及技术管理信息系统）。

8. 通用技术流程实施

17 个通用技术流程分别在不同小节描述, 包括开展经适当剪裁的所需流程活动的计划(所需流程活动及剪裁参见 NPR 7123.1)。17 个通用技术流程的实施包括(1)生成满足在 NPR 7123.1 中 D.4.4.4 中确定的相应相关产品寿命周期阶段的启动条件与成功准则所需的结果;(2)其他流程所需要的输入。这些小节中包含了对相应途径、方法和工具的描述:

- 确定并获得开展所计划流程, 开发工作产品, 并为流程提供服务的适当人力及非人力资源。
- 为执行所计划流程, 开发工作产品, 并为流程提供服务安排责任与权限。
- 培训技术人员开展并保障技术流程, 培训根据需要确定。
- 在技术状态管理适当的层次上指定并安排相应的流程工作产品。
- 确定流程涉及到的利益相关者。
- 对流程进行监督和控制。
- 确定、定义并追踪度量指标和成功准则。
- 客观评价流程、工作产品和服务与相应需求、目标和标准的一致程度, 说明不一致性。
- 从适当的管理层次上评审流程的活动、状态及结果, 并解决存在的问题。

本节还应该包含项目特定的对所用 17 个流程的描述, 包括对系统和项目需求的特定剪裁、流程实施所用的技术规程、内部文档、权衡研究方法、所用数学模型与仿真模型类型、规范的生成。

9. 技术引进

本节包含对于确定关键技术途径和方法及其用于评估和引进技术的相应风险和准则, 包括从技术开发项目中引入关键技术的风险和准则。应为确定技术引进的水平及时机开发相应的方法。这可能包括采用新技术的优势来满足系统需求的备选方法, 以及相关技术在结果上和时间内证明不合适时的替代选项。在项目需求的范围内, 应当提供初始技术评估策略, 以确定系统的技术约束。

10. 附加的系统工程功能与活动

本节包含对以上各节未专门描述的, 但对制定合适计划及实施整个技术工作是必不可少的其他领域的描述。

1) 系统安全性

本小节包含对进行安全性分析及评估人员、系统、环境或公共风险的途径和方法的描述。

2) 工程技术方法与工具

本节包含描述未包括在技术引入一节, 但需要支持整个技术工作的方法和工具, 并包含确定需要获取的工具及工具训练需求。

还应定义项目开发环境, 包括自动化和软件工具。如果需要, 应开发或获取项目中所有学科的工具和设备。可能时对项目标准化, 或保证工具的公共输出格式能用于项目所用大部分工具的输入。定义信息管理系统的需求及应用现有单元的需求。定义并计划在项目中应用工具及技术所需的培训。

3) 专业工程技术

本小节包含对应用于整个项目的工程技术学科和专业需求及系统结构的工作分解结构模型的描述。这些需求领域的实例包括安全性、可靠性、人因、后勤、维修性、质量、操作性及保障性。应估计技术人员的水平并结合到项目需求中。

11. 与项目计划集成和技术资源分配

本节包含技术工作如何与项目管理集成，并定义角色和责任。本节表述技术需求如何与项目计划集成以决定资源的分配，资源包括成本、进度、人员，还要确定分配的变更如何协调。

本节描述在系统工程计划活动和更新期间，项目所有技术方面与全面项目管理流程之间的接口。其中包含整个项目技术工作的所有协调活动，诸如与外部的利益相关者、用户及承包商的技术交流活动。

12. 免责声明

本节包含针对 NPR 7123.1 中系统工程管理计划需求的系统工程实施计划相应的所有经审批的免责声明。本节可包含若干小节，分别描述裁剪的 NPR 需求，这些需求互不相关并能归档为特定的系统工程管理计划中的小节。

13. 附录

根据需要包含附录，提供为方便文档维护而分别给出的术语表、首字母缩写和缩略语和其他信息。如此应包括（1）可有与多个主题领域相关的信息（如方法或技术规程的描述）；（2）可用于系统工程管理计划所需技术工作的图表和专用数据；（3）与项目相关的技术计划的总结。每一个附录都应在工程计划的某一部分引用，并提供正式的数据。

14. 模板

技术团队需要填写的相关表格、计划或报告的模板，如验证与确认计划的格式，应当在附录中说明。

15. 参考文献

本节包含在系统工程管理计划正文中所引用的所有文档。

16. 系统工程管理计划准备的清单

作为获取技术规划的关键参考文档，系统工程管理计划需要表述一些基本主题。一般系统工程管理计划应准备的清单，参见 James Martin 的《系统工程指导书》。

附录 K 计 划

活动计划	6.7
控制基线计划	111
建造计划	300
结束计划	178
技术状态管理计划	176, 311
费用记账计划	121
数据管理计划	158
部署计划	300
挣值管理计划	166
工程技术计划	附录 J
实施计划	148
安装计划	230
集成计划	299
接口控制计划	81
发射和早期轨道计划	35
寿命周期费用管理计划	129
后勤保障计划	26
使命任务实施计划	26
运行使用计划	35
生产计划	25
工程计划	19
项目计划	112
项目保护计划	260, 321
质量控制计划	24
需求管理计划	134
评审计划	169
风险控制计划	142
风险管理计划	140
风险缩减计划	295
软件开发计划	104
软件集成验证确认计划	105
来源评价计划	219
战略计划	152
监督计划	225
系统和子系统试验计划	42
系统退役/处置计划	113, 303

系统工程管理计划	2.0
技术开发计划	277
试验计划	230
按时间分段资源计划	190
交付计划	230
运输计划	187
确认计划	100, 284
验证计划	83

附录 L 接口需求文档概要

1. 引言

- 1.1 目的和范围。**阐述本文档的目的并简要辨识需要定义的接口（例如，“此接口需求文档定义和控制____和____之间的接口需求。”）。
- 1.2 优先权。**定义本文档与计划的其他文档的关系，并指定在发生冲突事件时哪一个文档有控制权。
- 1.3 责任和变更授权。**阐述开发此文档中接口及其内容相关组织的责任。定义文档批准权限（包括变更批准权限）。

2. 文档

- 2.1 适用文档。**列出本接口需求文档规定的范围内引用的书面文件。应当列出最终的修订本和最新版本。更高层次（高阶优先权）的文档中引用的文档和提出的需求不应重复。
- 2.2 参考文档。**列出在本小节中参考的所有文档。

3. 接口

- 3.1 总体。**在本小节中，详细提供接口界面相关的接口描述、职责、相关系统和数字化需求。
 - 3.1.1 接口描述。**描述在系统规范中定义的接口。适当使用表格、图形和示意图。
 - 3.1.2 接口职责。**定义刻画接口界面的接口硬件和接口边界职责。适当使用表格、图形和示意图。
 - 3.1.3 相关系统。**定义在接口的每个端口上接口需求相应的系统。适当使用表格、图形和示意图。
 - 3.1.4 工程单位、公差和转换。**定义度量单位及其公差。如果需要，定义度量体制之间的转换。
- 3.2 接口需求。**在本小节中，定义接口的结构限定值，如接口载荷、加载函数和动态条件。
 - 3.2.1 接口界面。**在接口界面的每个端口定义接口需求。
 - 3.2.1.1 包络**
 - 3.2.1.2 质量属性。**定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本节应当涵盖单元的质量。
 - 3.2.1.3 结构/力学属性。**定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖附件、硬度、锁闭和机构。
 - 3.2.1.4 流体属性。**定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖流体范围如热力学控制、O₂ 和 N₂、饮用水和污水、燃料供给和大气采样。
 - 3.2.1.5 电（力）属性。**定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖各类电流、电压、电功率和电阻水平。

3.2.1.6 电（信号）属性。定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖各种信号类型如音频、视频、控制指令数据及导航指令数据。

3.2.1.7 软件和数据。定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖各类数据标准、信息同步、协议、错误诊断/修正、功能、初始化和状态。

3.2.1.8 环境。定义基于需求分配得到的接口需求，该需求包含在接口端口适用的规范中。例如，本小节应当涵盖本接口端口上英制度量或等价公制度量单元的动态包络。

3.2.1.8.1 电磁影响

3.2.1.8.1.a 电磁兼容性。定义适当的电磁兼容性需求。例如，产品 1 与产品 2 的接口应当满足系统电磁兼容性需求中的某项（待定）需求。

3.2.1.8.1.b 电磁干扰。定义适当的电磁干扰需求。例如，产品 1 与产品 2 的接口应当满足系统电磁兼容性需求中的电磁发射和磁化率方面的某项（待定）需求。

3.2.1.8.1.c 接地。定义适当的接地需求。例如，产品 1 与产品 2 的接口应当满足某项（待定）接地需求。

3.2.1.8.1.d 连接。定义适当的连接需求。例如，产品 1 与产品 2 的接口应当满足电路连接需求的某项（待定）需求。

3.2.1.8.1.e 电缆和电线设计。定义适当的电缆和电线设计需求。例如，产品 1 与产品 2 的接口应当满足电磁兼容性需求的某项（待定）电缆/电线设计和控制需求。

3.2.1.8.2 声学。定义适当的声学需求。根据计划或项目需求定义每个接口端口的噪声水平。

3.2.1.8.3 结构载荷。定义适当的结构载荷需求。定义每个产品必须能够承受的载荷。

3.2.1.8.4 振动声学。定义适当的振动声学需求。定义每个产品必须能够承受的振动声学载荷。

3.2.1.9 其他类型的接口需求。定义其他类型可能适用的独立的接口需求。

附录 M 技术状态管理（CM）计划概要

典型的技术状态管理计划应当包含以下的内容。

表 M-1 技术状态管理概要

章 节	描 述
1.0 引言	本节包括的内容如下： <ul style="list-style-type: none">• 技术状态管理的目的和范围，及其计划中的应用阶段；• 系统或顶层状态控制项的简要描述
2.0 适用文档和参考文档	本节包括在计划中参考引用的规范、标准、指南和其他文件的列表，格式为标题、文献号、发行机构、版本及可能的变更通告、修正、发行日期
3.0 技术状态管理构想和组织	本节包括的内容如下： <ul style="list-style-type: none">• 技术状态管理目标；• 在当前和未来阶段中达到该目标所需要的信息；• 描述或图示强调技术状态管理活动的项目所规划的组织结构
4.0 技术状态管理流程 <ul style="list-style-type: none">• 技术状态管理与规划• 技术状态辨识• 技术状态控制• 技术状态状况统计• 技术状态审核	本节描述实现 5 个技术状态管理活动的项目技术状态管理流程，包括但不限于以下内容： <ul style="list-style-type: none">• 当前阶段和未来阶段的技术状态管理活动；• 控制基线；• 状态控制项；• 技术状态控制委员会的组建和成员；• 系统命名和编号；• 硬件和软件标识；• 功能技术状态审核和物理技术状态审核
5.0 技术状态数据的管理	本节描述满足技术状态管理数据需求的方法
6.0 接口管理	本节包括对技术状态管理如何维护和控制接口文档的描述
7.0 技术状态管理阶段和进度	本节描述与主计划里程碑对应的实施技术状态管理的里程碑
8.0 分包商/供货商控制	本节描述用于确保分包商/供货商遵从技术状态管理需求的方法

附录 N 技术同行评审/检查

1. 引言

技术同行评审/检查的目标是在系统开发过程中尽可能早地去除缺陷。同行评审/检查是发现并定位缺陷的良好的评审流程，由派定角色的一组同行执行，每个人关注待评审工作产品的既定方面。同行评审/检查针对已完成或部分完成的产品，在开发阶段进行，介于里程碑评审之间。同行评审/检查的结果可以在里程碑评审中报告。在同行评审/检查中充分应用清单，以提高评审的质量。

长期以来，技术同行评审/检查已被证明是确保产品质量及保证按时交付的最有效方法之一。在 NASA 内部和工业界，许多研究已经证明其价值。同行评审/检查通过减少重复工作提升质量和降低成本。研究表明，减少重复工作不仅对减少检查上的开销有益，还对节省项目成本有益。通过从根源上（如需求和设计文档、试验计划与技术规程、软件代码等）去除缺陷，这种检查可以阻止缺陷在多个阶段和工作产品中传播，并减少项目中需要的重复工作总量。另外，提高团队效率是同行评审/检查的附加效益（如加强团队交流，使新成员更快地融入角色，向项目人员传授高效的开发经验等）。

2. 如何开展技术同行评审/检查

图 N-1 给出同行评审/检查的阶段图，后文解释各个阶段评审如何执行（本附录最后的图 N-2 总结了相应信息，作为快速参考指南）。

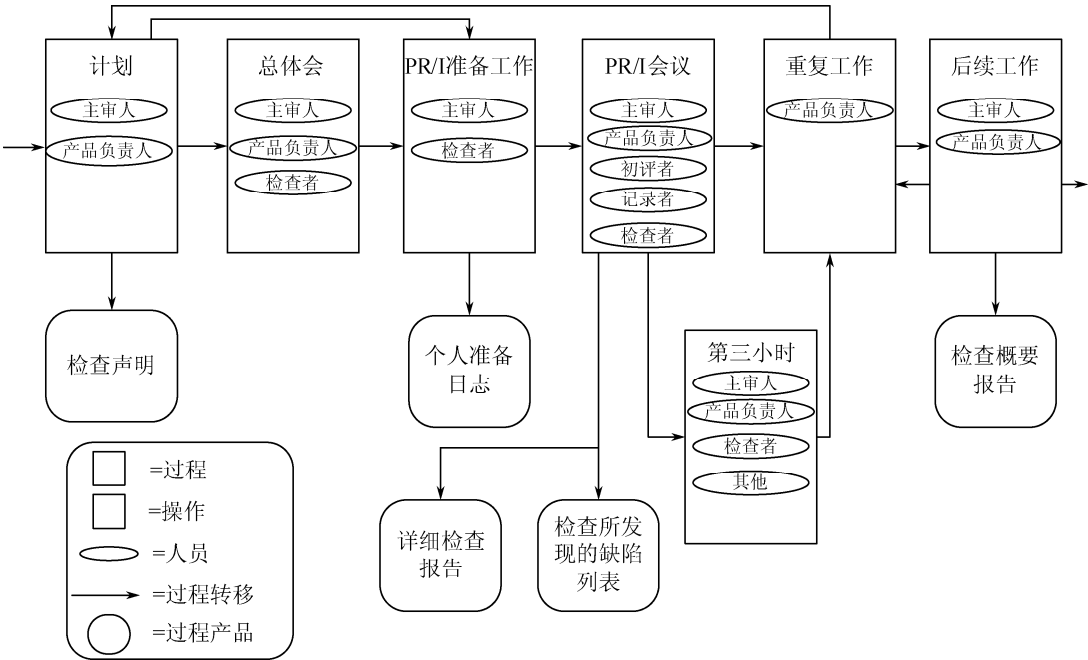


图 N-1 同行评审/检查流程

建议主审人在计划阶段开始前参阅图 N-2 中的“计划检查进度和估算人工工时”、“成功检查指导”和“检查的 10 项基本规则”（注意：NPR 7150.2 《NASA 软件工程需求》定义了

NASA 总局针对软件开发的同行评审和检查的需求。NASA 同行评审/检查培训由 NASA 总工程师办公室负责)。

注：下文中含有*的活动，需要主审人在检查总结报告中记录时间。

A. 计划

同行评审/检查的主审人开展下列活动（来自 NASA 兰利研究中心的《正式检查指导手册》。该文件对如何开展技术同行评审/检查提供更详细的指导。同时提供上述同行评审/检查流程中使用的模板形式：检查通告、独立检查日志、检查缺陷列表、详细检查报告和检查总结报告）。

(1) 确定同行评审/检查是否满足启动准则。

(2) 决定是否需要产品概要评审。

(3) 选择同行评审/检查小组成员并分配角色。关于角色分配，见本附录图 N-2 中的“参与者角色”。评审人对工作产品有既得利益（如待评审材料影响的寿命周期方面的同行代表）。

(4) 确定产品的规模是否在检查类型对应的既定指针下（见图 N-2 中“会议定级指针”，其中描述每一种检查类型需检查的最优文本页数或代码行数）。如果产品超出预定的指针，应将产品分解并分别检查各个部分（强烈建议同行评审/检查会议不超过 2h）。

(5)（如果需要）计划安排概要评审。

(6) 计划安排同行评审/检查会议的时间地点。

(7) 准备并分发检查通告和材料。材料包括需要检查的产品及相应同行评审/检查的清单。

(8) 记录计划安排所花费的总时间。*

B. 概要评审会议

(1) 主审人召集会议，产品负责人向检查者汇报背景信息。

(2) 记录概要评审所花费的总时间。*

C. 同行评审/检查准备

(1) 检查人评审定义清单是否存在缺陷。

(2) 检查了解所需材料及可能的缺陷。

(3) 同行评审/检查中分配的角色准备。

(4) 完成并向主审人提交个人准备日志。

(5) 主审人检查所有个人准备日志并作出是否继续评审的决策，并组织检查会议。

(6) 记录准备工作所花费的总时间。*

D. 同行评审/检查会议

(1) 主审人介绍人员并明确同行评审/检查中的角色。

(2) 初评人以符合逻辑顺序的方式将工作产品呈现给同行评审/检查小组。

(3) 同行评审/检查人员针对所发现缺陷根据严重性、种类及形式进行分类（参见图 N-2 中“缺陷的分类”）。

(4) 记录员将主要和次要缺陷写入检查所发现缺陷列表中（主要/次要缺陷的定义参见图 N-2 中的“严重性”）。

(5) 重复 (1) 至 (4) 步，直到完成产品的评审。

(6) 如果出现明显差异，将其提交同行评审/检查人员。

(7) 在详细检查报告中汇总缺陷的数量及其分类。

(8) 决定是否需要重新检查即进入所谓“第三小时”。可选方式：微小缺陷（如红线标注的文档）在检查完毕后可直接交给产品负责人处理。

(9) 主审人获得产品负责人重新工作时间及完成日期的估计，适当时对行动内容做估计。

(10) 如果需要，主审人安排撰写变更请求和问题报告。

(11) 记录同行评审/检查会议花费的总时间。*

E. “第三小时”

(1) 完成安排行动内容并向产品负责人提供信息。

(2) 按产品负责人请求参加“第三小时”会议。

(3) 向协调者提交“第三小时”花费的总时间。*

F. 重复工作

(1) 产品负责人解决在检查缺陷列表中的所有主要缺陷。

(2) 次要或微小缺陷（不会引起错误执行），在时间和成本允许时根据产品负责人的意见解决。

(3) 记录检查缺陷列表中重复工作花费的总时间。

G. 后续工作

(1) 主审人证实所有的主要缺陷已更正，且没有引出新的缺陷。

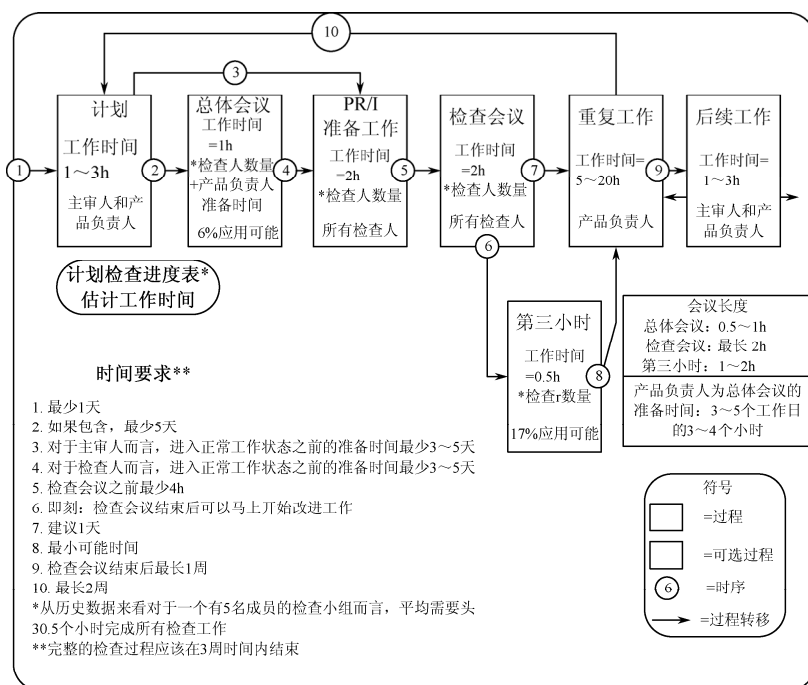
(2) 主审人确保所有未解决问题已被解决，并证实所有同行评审/检查的成功准则已满足。

(3) 记录重复工作与后续工作所花费的时间总和。*

(4) 将检查材料形成文件。

(5) 分发检查总结报告。

(6) 宣布同行评审/检查工作结束。



技术同行检查/评审

快速参考指导

检查的类型

SY1	系统需求
SY2	系统设计
SU1	子系统需求
SU2	子系统设计
R1	软件需求
10	架构设计
11	详细设计
12	源代码
IT1	试验计划
IT2	试验流程与功能

缺陷的分类

按严重程度

重大缺陷

- 引起多项功能失效的缺陷
- 在将来会导致不得不改变要求的缺陷

次要缺陷

- 对于标准、准则或者是规则的偏离, 即使不改正, 也不会导致与需求的偏离, 但是可能会在将来增加操作、保障、进一步开发工作的难度

微不足道的缺陷

- 诸如一些拼写、句点、语法错误, 不会引起不良后果, 这些缺陷只需要用红线标出, 直接呈现给产品负责人即可

产品负责人需要改正所有的重大缺陷, 根据成本和进度要求决定次要缺陷和微不足道的缺陷要不要改正

按类别目录

- 缺失
- 错误
- 多余

按类型

建议采用以下缺陷分类标准

- | | |
|----------|-------|
| ●清晰性 | ●接口 |
| ●完整性 | ●详细程度 |
| ●一致性 | ●保障性 |
| ●连贯性 | ●性能 |
| ●正确性/逻辑性 | ●可靠性 |
| ●可测试性 | ●数据效用 |
| ●可追溯性 | ●容错度 |
| ●功能性 | ●其他 |

实例

以下是在记录缺陷时将缺陷进行分类的实例

描述	分类
169行—	重大缺陷 <input checked="" type="checkbox"/> 该有的没有
.....	次要缺陷 <input type="checkbox"/> 错误 <input checked="" type="checkbox"/>
.....	冗余 <input type="checkbox"/>
.....	类型 <input type="text"/>
	来源 <input type="text"/>

实施成功检查的指导方针

- 对主审人、检查人和负责人进行相关的培训
- 检查时间不多于开发时间的25%
- 要对100%的产品进行检查
- 做好充分的准备
- 明确分工与职责
- 要注意进行良好的协作与沟通
- 避免武断的言语
- 不要对产品负责人品头论足
- 至少要有有一个积极的输入和消极的输入
- 只负责提出问题, 并不负责解决
- 避免风格方面的讨论
- 坚持标准, 要不就去改变它
- 技术上要能胜任
- 公开对所有问题进行记录
- 技术上的事宜要坚持
- 对于检查结果要及时地记录成文档
- 产品什么时候可以检查是产品负责人决定的
- 保持精确的统计

检查应遵循的10条规则

- 检查是在项目生命周期的各个阶段的不同节点上展开的, 它不可以代替里程碑检查
- 检查是由在项目中所受检查产品影响的部门技术人员实施的(通常6人以下), 这些检查人所在部门会受到产品质量的直接影响的
- 在检查中不存在管理工作, 检查不作为考核人员的依据
- 检查由一名受过培训的主审人总负责
- 为受过培训的检查人分配不同的角色
- 检查按照规定好的步骤展开
- 检查会议要在2h以内
- 问题清单用来定义任务并促进问题发现
- 检查会议期间要指定所有所需的材料, 从而使得具有最大的缺陷发现能力
- 统计缺陷的数目和缺陷的类型, 以及工程人员所花费的时间

对于不同的检查类型的会议*指导方针

类型	检查会议	
	目标/2h	范围/2h
R2	20页	10~30页
R1	20页	10~30页
10	30页	20~40页
11	35页	25~45页
12	500行代码**	400~600行代码**
IT1	30页	20~40页
IT2	35页	25~45页

*假设会议时间2小时, 对于小型产品的持续时间可以缩短

**飞行软件及其他高度复杂的代码段速率要求可以减半

参与者的角色

主审人

负责检查的全过程并收集检查数据, 在除去改进工作之外的所有阶段都起到至关重要的作用。在检查过程中, 需要执行一些特殊的使命

检查人

负责从通常的视角发现产品中存在的缺陷, 包括那些影响到其相关领域的缺陷

产品负责人

在检查过程中的所有阶段负责提供产品的相关信息, 负责收集产品的主要缺陷和微小缺陷及它们带来的成本和进度上的代价

初评人

在检查会议中对检查小组起到引导作用, 详细解释产品的有关细节在履行其基本职责之外还要承担一部分检查人的责任

记录人

确切地说, 他们的职责就是将发现的每一个缺陷记录下来成为清单, 在其基本职责之外还要履行检查人的职责

图 N-2 同行评审/检查快速参考指南

附录 O 权 衡 示 例

表 O-1 空间系统的典型权衡

研 发 相 关	使用与保障相关
<ul style="list-style-type: none">• 用户定制对比商用成品；• 轻便（贵重）部件对比沉重（便宜）部件；• 星上处理对比远程处理；• 无线频率对比光学链路；• 余量水平对比费用/风险分析；• 微小问题部件对比较大问题部件；• 抗辐射加固对比标准部件；• 冗余度；• 质保度；• 联机测试对比远程诊断；• 使用前环境暴露类型；• 试验水平（系统对比子系统）；• 各类寿命周期方法（如瀑布式对比螺旋式或对比递增式）	<ul style="list-style-type: none">• 升级型号对比新型号；• 载人对比无人；• 自主控制对比远程控制；• 体系对比单机系统；• 单个长寿命单元对比多个短寿命单元；• 地球低轨道对比地球中轨道或对比地球同步静止轨道或对比地球高轨道；• 单卫星对比星座；• 运载火箭类型（Atlas 对比 Titan）；• 单级发射对比多级发射；• 在轨维修对比返回地面维修；• 商用设施对比政府资产；• 限制访问对比公开访问；• 可控返回对比不可控返回

表 O-2 采办过程中的典型权衡

采 办 阶 段	权衡研究目的
使命需求分析	确定用户需求的优先次序
概念探索（概念和技术开发）	<ul style="list-style-type: none">（1）对比新技术与已验证概念；（2）选择最佳满足使命需求的概念；（3）选择备选系统技术状态；（4）聚焦可行性和负担能力
演示验证/确认	<ul style="list-style-type: none">（1）选择技术；（2）备选技术状态缩减到可测数量
全尺寸研发（系统研发和演示验证）	<ul style="list-style-type: none">（1）选择组件/部件设计方案；（2）选择试验方法；（3）选择使用试验和评价指标量
生产	<ul style="list-style-type: none">（1）检查所有设计变更提议的效能；（2）进行制造/购买、工序、比例和场所的决策

表 O-3 贯穿项目寿命周期的典型权衡

A 前 阶 段	阶 段 A	阶 段 B
<ul style="list-style-type: none">• 问题选定；• 升级对比新型号	<ul style="list-style-type: none">• 星上处理对地面处理；• 低地球轨道对比地球静止轨道	<ul style="list-style-type: none">• 冗余度；• 无线频率链路对比光学链路
阶段 C 和阶段 D	阶段 D 和阶段 E	阶段 E 和阶段 F
<ul style="list-style-type: none">• 单源对比多源；• 试验水平	<ul style="list-style-type: none">• STS-28 平台对比 STS-3a 平台；• 发射权衡（发射或不发射）	<ul style="list-style-type: none">• 轨道每日修正对比每周修正；• 当前变轨对比稍后变轨

附录 P 任务书（SOW）评审清单

1. 清单的格式

（1）任务书需求是“谁”需要“做什么”形式吗？例如，“承包商需要（开展、提供、开发、试验、分析或其他动词，接对‘什么’的描述）。 ”

任务书需求的示例：

- 承包商需要设计 XYZ 飞行软件……
- 承包商需要使用 ABC 地面系统……
- 承包商需要为以下系统提供维护……
- 承包商需要每月报告软件指标……
- 承包商需要把 PQR 仪器与航天飞行器集成……

（2）任务书需求是仅包含一个需求的简单语句吗？

包含多个任务书需求的复合句应当拆成若干简单语句（例如，“承包商需要做 ABC 并开展 XYZ”应当重写为“承包商需要做 ABC”和“承包商需要开展 XYZ”）。

（3）任务书是否由简单、紧凑的段落组成，且每段仅包含一个主题？包含多个需求的段落应当分为子段落。

（4）是否每个段落或子段落有独自的数字或字母标识？数字或字母标识是否正确？

（5）任务书需求是否以主动而非被动语态给出？被动语态可能导致模糊陈述（例如，用陈述“承包商需要每月举行管理评审会议”替代“管理评审会议需要每月举行”）。

（6）任务书需求是否正面陈述而非负面陈述（例如，用陈述“承包商必须遵从指定的预算限制”替代“承包商不应超出指定的预算限制”）？

（7）任务书需求在语法上是否正确？

（8）任务书需求是否清除打字、拼写及标点错误？

（9）是否已定义首字母缩写清单或在其首次出现时给出完整拼写？

（10）任务书中每个交付件是否已明确数量、交付计划及交付方法，或在附件中单独给出？

（11）需要交付的文档内容是否已分别在附件中定义，并与任务书共同提交？

（12）以电子版形式交付的文件是否已定义格式（例如，Microsoft 的 project，Adobe 的 Acrobat PDF，National Instruments 的 Lab view VIs）？

2. 清单的内容

（1）是否使用正确术语定义需求？

- 需要=需求（约束承包商）；
- 应当=目标（由承包商决策，避免使用该词）；
- 可以=合适行动（由承包商决策，避免使用该词）；
- 要求=政府意图的事实或声明（仅用于与政府有关的内容）；
- 现在时（如“is”）=仅描述性文本（避免在需求陈述中应用，用“需要”陈述代替）；
- 绝不使用“必须”。

(2) 任务书范围是否明确界定？是否清楚要买什么？

(3) 文档的流程与组织结构是否符合逻辑并易于理解（参见 LPR5000.2《采购发起者指导》第 12 节获得帮助）？文本内容是否与节标题一致？副标题与主标题是否一致？

(4) 任务书需求是否清晰且易于理解？

- 每个语句是否只有一个含义？
- 所有未定义术语对不同读者含义是否相同？是否有术语含义与任务书中定义的不同（如在定义段或词汇表中）？
- 是否清除未提前说明的不定代词（“这个”、“那个”、“这些”、“那些”）（如“这些应当每年检查”替换为“风机叶片应当每年检查”）？
- 陈述是否简明？

(5) 是否已去除冗余的需求？冗余需求会降低清晰性，增加模糊性，并导致矛盾的出现。

(6) 需求是否与任务书中其他需求一致，没有自相矛盾，没有用同一术语表达不同含义，没有用不同术语表达同一含义？

(7) 若任务书包含产品交付（相对仅有服务的任务书）：

- 技术产品需求是否在单独节或附录中，与承包商需要开展的活动相分离？目的是否清晰地描绘出技术产品需求与承包商需要开展的活动需求之间的不同（例如，任务书中“承包商需要”陈述与技术产品需求陈述如“系统需要”或“软件需要”区分开来）。
- 任务书中产品及其子单元的参考是否处在技术产品需求描述的层次上？
- 任务书是否使用相同的术语表述技术产品需求并保持一致？

(8) 任务书需求是否没有歧义？确保任务书需求没有模糊的词汇（如“适当时”、“任何”、“任一”、“等等”、“和/或”、“支持”、“必要”、“但不限于”、“可以”、“能够”）。

(9) 任务书需求是否可证实？确保任务书需求中没有不可证实的词语（如“灵活”、“简便”、“充分”、“安全”、“特别”、“足够”、“满足”、“界面友好”、“可用”、“需要时”、“若需要”、“合适”、“快捷”、“可移植”、“轻便”、“小的”、“大的”、“最大”、“最小”、“最优”、“鲁棒”、“快速”、“容易”、“清晰”及其他类似词汇）。

(10) 任务书需求是否没有实施限制？任务书需求应该陈述承包商做什么，而不是他们如何做（如“承包商需要设计 XYZ 飞行软件”陈述承包商做什么，而“承包商需要用面向对象设计方法设计 XYZ 飞行软件”则陈述承包商如何实施软件设计活动。另外，活动分解层次过低，可能导致指定活动如何完成而不是完成什么活动）。

(11) 任务书需求是否以遵从需求可验证的方式陈述？度量抑或评价其完成的手段是否存在？验证的方法是否遵从所定义（如在质量保证监督计划中所描述）的需求？

(12) 背景材料是否被清晰标注（如需要时包含在任务书的背景章节）？

(13) 所有假设是否能作为需求被确认并重申？若否，假设应当从任务书中删除。假设应当记录在与任务书分离的文档中。

(14) 任务书是否完整，覆盖承包商应做的所有工作？

- 是否包括开发产品需要的所有活动（如系统、软件、硬件的下列活动：需求、构架与设计开发；实施与制造；验证与确认；集成试验与合格试验）？
- 是否针对合同全寿命定义安全性、可靠性、维修性（如平均修复时间）、可用性、质量保证及安全需求？

- 如果需要, 任务书中是否包括对承包商的质量体系 (如 ISO 认证) 的需求?
- 是否所有管理和保障需求包含在任务书中 (如项目管理; 技术状态管理; 系统工程; 系统集成与试验; 风险管理; 接口定义与管理; 指标值采集、报告、分析与使用; 验收试验; NASA 独立验证与确认保障任务)?
- 性能标准能否充分度量承包商的绩效 (如针对进度、进展、规模、稳定性、成本、资源及缺陷的系统、软件、硬件和服务性能标准)? 参见 NASA 兰利中心的《系统和软件合同性能指标指南》获取更多信息和实例。
- 是否包括所有需要的服务活动 (如交付使用、运行使用、维护、数据库管理、系统管理及数据管理)?
- 是否包括所有政府监管活动 (如项目管理会议, 决策点, 系统、软件、硬件需求和设计同行评审, 演示验证, 试验准备状态评审, 其他必要的会议 (如技术交流会议), 系统、软件、硬件和服务指标的采集与分发 (提高开发进展及成本的清晰度), 技术数据与管理数据的电子访问, 以交流为目的访问分包商及团队成员)?
- 需要时, 是否表述政府对承包商的检查试验需求?
- 需要时, 是否表述承包商保障政府验收活动的需求?

(15) 任务书是否仅包括承包商需求? 它不应当包括对政府方面的需求。

(16) 任务书是否给予承包商完全管理责任, 并使他们对最终结果承担责任?

(17) 任务书是否足够详细, 以便对完成每项活动需要的成本、劳力及其他资源做实际估算?

(18) 所有交付件是否确定 (如状态、财政、产品交付件)? 以下是有时被忽略的交付件: 管理与开发计划, 确定当前工作状态、问题及纠正行动建议、计划工作的技术进展报告, 分类确定 (计划、实际、规划) 成本的财务报告, 产品 (源代码、维护/用户手册、试验设备), 偏差数据 (如缺陷报告、异常)。除了技术交付件 (如硬件、软件、原型) 应当包括在任务书中之外, 所有交付件应当在单独的文档中确定。

(19) 是否每个技术与管理交付件都可以在任务书中追溯到段落? 每个交付件应当有相应的任务书需求作预备 (即任务需要生成交付件时应在任务书中标识交付件)。

(20) 所有的参考引文是否完整?

- 参考文献的标号、标题、日期或版本是否完整?
- 任务书是否在适当的段落中参考标准和其他相应文档?
- 参考文档是否被正确引用且至少引用一次?
- 参考文档是否列入任务书或可在任务书指定的位置获得?
- 如果参考的标准或相应文档只是部分可用, 任务书中是否明确无歧义地指出承包商所需参考的部分?

附录 Q 项目防护规划概要

下列概要帮助系统工程师制定项目防护规划。该规划是一个动态文件，在项目经历主要里程碑及最终项目结束时撰写和更新。

1. 引言

- 1.1 防护规划概述
- 1.2 项目概述
- 1.3 采办状态

2. 参考

- 2.1 指示和指令
- 2.2 需求
- 2.3 研究与分析

3. 参考

- 3.1 威胁：敌意行动
 - 3.1.1 概述
 - 3.1.2 威胁特征
 - 3.1.2.1 网络攻击
 - 3.1.2.2 电子攻击
 - 3.1.2.3 激光
 - 3.1.2.4 地面攻击
 - 3.1.2.5 对关键商业基础设施的非对称攻击
 - 3.1.2.6 反卫星武器
 - 3.1.2.7 高能电磁辐射武器
 - 3.1.2.8 人工增强的辐射环境
- 3.2 威胁：环境
 - 3.2.1 概述
 - 3.2.2 威胁特征
 - 3.2.2.1 自然环境风暴
 - 3.2.2.2 地震
 - 3.2.2.3 洪水
 - 3.2.2.4 火灾
 - 3.2.2.5 自然环境的辐射影响
 - 3.2.2.6 对航天器电子辐射影响

4. 防护脆弱性

- 4.1 地面装备的脆弱性
 - 4.1.1 指挥与控制设施
 - 4.1.2 远程跟踪站
 - 4.1.3 航天飞行器模拟器
 - 4.1.4 使命任务数据处理设施

- 4.1.5 飞行动力学设施
- 4.1.6 飞行软件产品/验证/确认设施
- 4.2 通信/信息装备脆弱性
 - 4.2.1 指挥链路
 - 4.2.2 遥测链路（使命任务数据）
 - 4.2.3 遥测链路（工程数据）
 - 4.2.4 地面网络
- 4.3 空间装备脆弱性
 - 4.3.1 航天飞行器物理特性
 - 4.3.2 航天飞行器使用特性
 - 4.3.3 轨道参数
 - 4.3.4 光学设备（传感器/传输器/接收器）
 - 4.3.5 通信子系统
 - 4.3.6 指挥与数据管理子系统
 - 4.3.7 仪器
- 4.4 发射装备脆弱性
 - 4.4.1 发射参数
 - 4.4.2 发射场集成与试验活动
- 4.5 商业基础设施脆弱性
 - 4.5.1 电能
 - 4.5.2 天然气
 - 4.5.3 远程通信
 - 4.5.4 运输
- 5. 防护对策**
 - 5.1 防护策略
 - 5.2 使命任务威胁减缓
 - 5.3 使命任务恢复选择
 - 5.4 使命任务生存特征
- 6. 碎片风险缓解**
 - 6.1 设计方针
 - 6.2 致命性减缓规程
 - 6.3 防撞
- 7. 关键工程信息和技术**
 - 7.1 关键工程信息单元
 - 7.2 关键信息计划
- 8. 工程防护成本**
 - 8.1 系统权衡分析
 - 8.2 成本/收益分析

分章节参考文献

第 2 章 系统工程基础

Griffin, Michael D., *System Engineering and the Two Cultures of Engineering*. 2007.

Rechtin, Eberhardt. *Systems Architecting of Organizations: Why Eagles Can't Swim*. 2000.

3.4 项目阶段 A: 概念和技术开发

NASA. *NASA Safety Standard 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris*. 1995.

4.1 明确利益相关者期望

ANSI. *Guide for the Preparation of Operational Concept Documents*. 1992.

4.2 技术需求定义

NASA. *NASA Space Flight Human System Standard*. 2007.

4.3 逻辑分解

Institute of Electrical and Electronics Engineers. *Standard Glossary of Software Engineering Terminology*. 1999.

4.4 设计方案

Blanchard, Benjamin S. *System Engineering Management*. 2006.

DOD. *MIL-STD-1472, Human Engineering*. 2003.

Federal Aviation Administration. *Human Factors Design Standard*. 2003.

International Organization for Standardization. *Quality Systems Aerospace—Model for Quality Assurance in Design, Development, Production, Installation, and Servicing*. 1999.

NASA. *NASA Space Flight Human System Standard*. 2007.

NASA. *Planning, Developing and Maintaining an Effective Reliability and Maintainability (R&M) Program*. 1998.

U. S. Army Research Laboratory. *MIL HDBK 727, Design Guidance for Producibility*. 1990.

U.S. Nuclear Regulatory Commission. *Human-System Interface Design Review Guidelines*. 2002.

5.1 产品实施

American Institute of Aeronautics and Astronautics. *AIAA Guide for Managing the Use of Commercial Off the Shelf (COTS) Software Components for Mission-Critical Systems*. 2006.

International Council on Systems Engineering. *Systems Engineering Handbook*. 2006.

NASA. *Off-the-Shelf Hardware Utilization in Flight Hardware Development*. 2004.

5.3 验证

Electronic Industries Alliance. *Processes for Engineering a System*. 1999.

Institute of Electrical and Electronics Engineers. *Standard for Application and Management of the Systems*

Engineering Process. 1998.

International Organization for Standardization. *Systems Engineering—System Life Cycle Processes*. 2002.

NASA. *Project Management: Systems Engineering & Project Control Processes and Requirements*. 2004.

U.S. Air Force. *SMC Systems Engineering Primer and Handbook*. 2005.

5.4 确认

Electronic Industries Alliance. *Processes for Engineering a System*. 1999.

Institute of Electrical and Electronics Engineers. *Standard for Application and Management of the Systems Engineering Process*. 1998.

International Organization for Standardization. *Systems Engineering—System Life Cycle Processes*. 2002.

NASA. *Project Management: Systems Engineering & Project Control Processes and Requirements*. 2004.

U.S. Air Force. *SMC Systems Engineering Primer and Handbook*. 2005.

5.5 产品交付

DOD. *Defense Acquisition Guidebook*. 2004.

Electronic Industries Alliance. *Processes for Engineering a System*. 1999.

International Council on Systems Engineering. *Systems Engineering Handbook*. 2006.

International Organization for Standardization. *Systems Engineering—A Guide for the Application of ISO/IEC 15288*. 2003.

—. *Systems Engineering—System Life Cycle Processes*. 2002.

Naval Air Systems Command. *Systems Command SE Guide: 2003*. 2003.

6.1 技术规划

American Institute of Aeronautics and Astronautics. *AIAA Guide for Managing the Use of Commercial Off the Shelf (COTS) Software Components for Mission-Critical Systems*. 2006.

Institute of Electrical and Electronics Engineers. *Standard for Application and Management of the Systems Engineering Process*. 1998.

Martin, James N. *Systems Engineering Guidebook: A Process for Developing Systems and Products*. 1996.

NASA. *NASA Cost Estimating Handbook*. 2004.

—. *Standard for Models and Simulations*. 2006.

6.4 技术风险管理

Clemen, R., and T. Reilly. *Making Hard Decisions with DecisionTools Suite*. 2002.

Dezfuli, H. “Role of System Safety in Risk-Informed Decisionmaking.” 2005.

Kaplan, S., and B. John Garrick. “On the Quantitative Definition of Risk.” 1981.

Morgan, M. Granger, and M. Henrion. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. 1990.

Stamelatos, M., H. Dezfuli, and G. Apostolakis. “A Proposed Risk-Informed Decisionmaking Framework for NASA.” 2006.

Stern, Paul C., and Harvey V. Fineberg, eds. *Understanding Risk: Informing Decisions in a Democratic Society*. 1996.

U.S. Nuclear Regulatory Commission. *White Paper on Risk-Informed and Performance-Based Regulation*. 1998.

6.5 技术形态管理

American Society of Mechanical Engineers. *Engineering Drawing Practices*. 2004.

—. *Types and Applications of Engineering Drawings*. 1999.

DOD. *Defense Logistics Agency (DLA) Cataloging Handbook*.

—. *MIL-HDBK-965, Parts Control Program*. 1996.

—. *MIL-STD-881B, Work Breakdown Structure (WBS) for Defense Materiel Items*. 1993.

DOD, U.S. General Services Administration, and NASA. *Acquisition of Commercial Items*. 2007.

—. *Quality Assurance, Nonconforming Supplies or Services*. 2007.

Institute of Electrical and Electronics Engineers. *EIA Guide for Information Technology Software Life Cycle Processes—Life Cycle Data*. 1997.

—. *IEEE Guide to Software Configuration Management*. 1987.

—. *Standard for Software Configuration Management Plans*. 1998.

International Organization for Standardization. *Information Technology—Software Life Cycle Processes Configuration Management*. 1998.

—. *Quality Management—Guidelines for Configuration Management*. 1995.

NASA. *NOAA-N Prime Mishap Investigation Final Report*. 2004.

National Defense Industrial Association. *Data Management*. 2004.

—. *National Consensus Standard for Configuration Management*. 1998.

6.6 技术数据管理

National Defense Industrial Association. *Data Management*. 2004.

—. *National Consensus Standard for Configuration Management*. 1998.

6.8 决策分析

Blanchard, Benjamin S. *System Engineering Management*. 2006.

Blanchard, Benjamin S., and Wolter Fabrycky. *Systems Engineering and Analysis*. 2006.

Clemen, R., and T. Reilly. *Making Hard Decisions with DecisionTools Suite*. 2002.

Keeney, Ralph L. *Value-Focused Thinking: A Path to Creative Decisionmaking*. 1992.

Keeney, Ralph L., and Timothy L. McDaniels. “A Framework to Guide Thinking and Analysis Regarding Climate Change Policies.” 2001.

Keeney, Ralph L., and Howard Raiffa. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. 1993.

Morgan, M. Granger, and M. Henrion. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. 1990.

Saaty, Thomas L. *The Analytic Hierarchy Process*. 1980.

7.1 与合同相关的工程技术

- Adams, R. J., S. Eslinger, P. Hantos, K. L. Owens, et al. *Software Development Standard for Space Systems*. 2005.
- DOD, U.S. General Services Administration, and NASA. *Contracting Office Responsibilities*. 2007.
- Eslinger, Suellen. *Software Acquisition Best Practices for the Early Acquisition Phases*. 2004.
- Hofmann, Hubert F., Kathryn M. Dodson, Gowri S. Ramani, and Deborah K. Yedlin. *Adapting CMMI? for Acquisition Organizations: A Preliminary Report*. 2006.
- International Council on Systems Engineering. *Systems Engineering Handbook: A "What To" Guide for all SE Practitioners*. 2004.
- The Mitre Corporation. *Common Risks and Risk Mitigation Actions for a COTS-Based System*.
- NASA. *Final Memorandum on NASA's Acquisition Approach Regarding Requirements for Certain Software Engineering Tools to Support NASA Programs*. 2006.
- . *The SEB Source Evaluation Process*. 2001.
- . *Solicitation to Contract Award*. 2007.
- . *Standard for Models and Simulations*. 2006.
- . *Statement of Work Checklist*.
- . *System and Software Metrics for Performance-Based Contracting*.
- Naval Air Systems Command. *Systems Engineering Guide*. 2003.

7.2 一体化设计平台

- Miao, Y., and J. M. Haake. "Supporting Concurrent Design by Integrating Information Sharing and Activity Synchronization." 1998.

7.4 人因工程

- Blanchard, Benjamin S., and Wolter Fabrycky. *Systems Engineering and Analysis*. 2006.
- Chapanis, A. "The Error-Provocative Situation: A Central Measurement Problem in Human Factors Engineering." 1980.
- DOD. *Human Engineering Procedures Guide*. 1987. —. *MIL-HDBK-46855A, Human Engineering Program Process and Procedures*. 1996.
- Eggemeier, F. T., and G. F. Wilson. "Performance and Subjective Measures of Workload in Multitask Environments." 1991.
- Endsley, M. R., and M. D. Rogers. "Situation Awareness Information Requirements Analysis for En Route Air Traffic Control." 1994.
- Fuld, R. B. "The Fiction of Function Allocation." 1993.
- Glass, J. T., V. Zaloom, and D. Gates. "A Micro-Computer-Aided Link Analysis Tool." 1991.
- Gopher, D., and E. Donchin. "Workload: An Examination of the Concept." 1986.
- Hart, S. G., and C. D. Wickens. "Workload Assessment and Prediction." 1990.
- Huey, B. M., and C. D. Wickens, eds. *Workload Transition*. 1993.
- Jones, E. R., R. T. Hennessy, and S. Deutsch, eds. *Human Factors Aspects of Simulation*. 1985.
- Kirwin, B., and L. K. Ainsworth. *A Guide to Task Analysis*. 1992.
- Kurke, M. I. "Operational Sequence Diagrams in System Design." 1961.

- Meister, David. *Behavioral Analysis and Measurement Methods*. 1985.
- . *Human Factors: Theory and Practice*. 1971.
- Price, H. E. “The Allocation of Functions in Systems.” 1985.
- Shafer, J. B. “Practical Workload Assessment in the Development Process.” 1987.

7.6 度量单位的使用

- DOD. *DoD Guide for Identification and Development of Metric Standards*. 2003.
- Taylor, Barry. *Guide for the Use of the International System of Units (SI)*. 2007.

附录 F 功能、时间和状态分析

- Buede, Dennis. *The Engineering Design of Systems: Models and Methods*. 2000.
- Defense Acquisition University. *Systems Engineering Fundamentals Guide*. 2001.
- Long, Jim. *Relationships Between Common Graphical Representations in Systems Engineering*. 2002.
- NASA. *Training Manual for Elements of Interface Definition and Control*. 1997.
- Sage, Andrew, and William Rouse. *The Handbook of Systems Engineering and Management*. 1999.

附录 H 集成计划大纲

- Federal Highway Administration and CalTrans. *Systems Engineering Guidebook for ITS*. 2007.

附录 J 系统工程管理计划内容 SEMP 大纲

- DOD. *MIL-HDBK-881, Work Breakdown Structures for Defense Materiel Systems*. 2005.
- DOD Systems Management College. *Systems Engineering Fundamentals*. 2001.
- Martin, James N. *Systems Engineering Guidebook: A Process for Developing Systems and Products*. 1996.
- NASA. *NASA Cost Estimating Handbook*. 2004.
- The Project Management InstituteR. *Practice Standards for Work Breakdown Structures*. 2001.

按作者参考文献

- Adams, R. J., et al. *Software Development Standard for Space Systems*, Aerospace Report No. TOR—2004(3909)-3537, Revision B. March 11, 2005.
- American Institute of Aeronautics and Astronautics. *AIAA Guide for Managing the Use of Commercial Off the Shelf (COTS) Software Components for Mission-Critical Systems*, AIAA G-118-2006e. Reston, VA, 2006.
- American National Standards Institute. *Guide for the Preparation of Operational Concept Documents*, ANSI/AIAA G-043-1992. Washington, DC, 1992.
- American Society of Mechanical Engineers. *Engineering Drawing Practices*, ASME Y14.100. New York, 2004.
- . *Types and Applications of Engineering Drawings*, ASME Y14.24. New York, 1999.
- Blanchard, Benjamin S. *System Engineering Management*, 6th ed. New Dehli: Prentice Hall of India Private Limited, 2006.
- Blanchard, Benjamin S., and Wolter Fabrycky. *Systems Engineering and Analysis*, 6th ed. New Dehli: Prentice Hall of India Private Limited, 2006.
- Buede, Dennis. *The Engineering Design of Systems: Models and Methods*. New York: Wiley & Sons, 2000.
- Chapanis, A. “The Error-Provocative Situation: A Central Measurement Problem in Human Factors Engineering.” In *The Measurement of Safety Performance*. Edited by W. E. Tarrants. New York: Garland STPM Press, 1980.
- Clemen, R., and T. Reilly. *Making Hard Decisions with DecisionTools Suite*. Pacific Grove, CA: Duxbury Resource Center, 2002.
- Defense Acquisition University. *Systems Engineering Fundamentals Guide*. Fort Belvoir, VA, 2001.
- Department of Defense. *DOD Architecture Framework, Version 1.5, Vol. 1*. Washington, DC, 2007.
- . *Defense Logistics Agency (DLA) Cataloging Handbook*, H4/H8 Series. Washington, DC.
- . *DoD Guide for Identification and Development of Metric Standards*, SD-10. Washington, DC: DOD, Office of the Under Secretary of Defense, Acquisition, Technology, & Logistics, 2003.
- . *DOD-HDBK-763, Human Engineering Procedures Guide*. Washington, DC, 1987.
- . *MIL-HDBK-965, Parts Control Program*. Washington, DC, 1996.
- . *MIL-HDBK-46855A, Human Engineering Program Process and Procedures*. Washington, DC, 1996.
- . *MIL-STD-881B, Work Breakdown Structure (WBS) for Defense Materiel Items*. Washington, DC, 1993.
- . *MIL-STD-1472, Human Engineering*. Washington, DC, 2003.
- DOD, Systems Management College. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Acquisition Press, 2001.
- DOD, U.S. General Services Administration, and NASA. *Acquisition of Commercial Items*, 14CFR1214—Part 1214—Space Flight 48CFR1814. Washington, DC, 2007.
- . *Contracting Office Responsibilities*, i 46.103(a). Washington, DC, 2007.
- . *Quality Assurance, Nonconforming Supplies or Services*, FAR Part 46.407. Washington, DC, 2007.
- Dezfuli, H. “Role of System Safety in Risk-informed Decisionmaking.” In *Proceedings, the NASA Risk Management Conference 2005*. Orlando, December 7, 2005.
- Eggemeier, F. T., and G. F. Wilson. “Performance and Subjective Measures of Workload in Multitask Environments.” In *Multiple-Task Performance*. Edited by D. Damos. London: Taylor and Francis, 1991.
- Electronic Industries Alliance. *Processes for Engineering a System*, ANSI/EIA-632. Arlington, VA, 1999.

- Endsley, M. R., and M. D. Rogers. "Situation Awareness Information Requirements Analysis for En Route Air Traffic Control." In *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting*. Santa Monica: Human Factors and Ergonomics Society, 1994.
- Eslinger, Suellen. *Software Acquisition Best Practices for the Early Acquisition Phases*. El Segundo, CA: The Aerospace Corporation, 2004.
- Federal Aviation Administration. HF-STD-001, *Human Factors Design Standard*. Washington, DC, 2003.
- Federal Highway Administration, and CalTrans. *Systems Engineering Guidebook for ITS*, Version 2.0. Washington, DC: U.S. Department of Transportation, 2007.
- Fuld, R. B. "The Fiction of Function Allocation." *Ergonomics in Design* (January 1993): 20–24.
- Glass, J. T., V. Zaloom, and D. Gates. "A Micro-Computer-Aided Link Analysis Tool." *Computers in Industry* 16, (1991): 179–87.
- Gopher, D., and E. Donchin. "Workload: An Examination of the Concept." In *Handbook of Perception and Human Performance: Vol. II. Cognitive Processes and Performance*. Edited by K. R. Boff, L. Kaufman, and J. P. Thomas. New York: John Wiley & Sons, 1986.
- Griffin, Michael D., NASA Administrator. "System Engineering and the Two Cultures of Engineering." Boeing Lecture, Purdue University, March 28, 2007.
- Hart, S. G., and C. D. Wickens. "Workload Assessment and Prediction." In *MANPRINT: An Approach to Systems Integration*. Edited by H. R. Booher. New York: Van Nostrand Reinhold, 1990.
- Hofmann, Hubert F., Kathryn M. Dodson, Gowri S. Ramani, and Deborah K. Yedlin. *Adapting CMMI? for Acquisition Organizations: A Preliminary Report*, CMU/SEI-2006-SR-005. Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2006, pp. 338–40.
- Huey, B. M., and C. D. Wickens, eds. *Workload Transition*. Washington, DC: National Academy Press, 1993.
- Institute of Electrical and Electronics Engineers. *EIA Guide for Information Technology Software Life Cycle Processes—Life Cycle Data*, IEEE Std 12207.1. Washington, DC, 1997.
- . *IEEE Guide to Software Configuration Management*, ANSI/IEEE 1042. Washington, DC, 1987.
- . *Standard for Application and Management of the Systems Engineering Process*, IEEE Std 1220. Washington, DC, 1998.
- . *Standard Glossary of Software Engineering Terminology*, IEEE Std 610.12-1990. Washington, DC, 1999.
- . *Standard for Software Configuration Management Plans*, IEEE Std 828. Washington, DC, 1998.
- International Council on Systems Engineering. *Systems Engineering Handbook*, version 3. Seattle, 2006.
- . *Systems Engineering Handbook: A "What To" Guide for All SE Practitioners*, INCOSE-TP-2003-016-02, Version 2a. Seattle, 2004.
- International Organization for Standardization. *Information Technology—Software Life Cycle Processes Configuration Management*, ISO TR 15846. Geneva, 1998.
- . *Quality Management—Guidelines for Configuration Management*, ISO 10007: 1995(E). Geneva, 1995.
- . *Quality Systems Aerospace—Model for Quality Assurance in Design, Development, Production, Installation, and Servicing*, ISO 9100/AS9100. Geneva: International Organization for Standardization, 1999.
- . *Systems Engineering—A Guide for the Application of ISO/IEC 15288*, ISO/IEC TR 19760: 2003. Geneva, 2003.
- . *Systems Engineering—System Life Cycle Processes*, ISO/IEC 15288: 2002. Geneva, 2002.
- Jones, E. R., R. T. Hennessy, and S. Deutsch, eds. *Human Factors Aspects of Simulation*. Washington, DC: National Academy Press, 1985.

- Kaplan, S., and B. John Garrick. "On the Quantitative Definition of Risk." *Risk Analysis* 1(1). 1981.
- Keeney, Ralph L. *Value-Focused Thinking: A Path to Creative Decisionmaking*. Cambridge, MA: Harvard University Press, 1992.
- Keeney, Ralph L., and Timothy L. McDaniels. "A Framework to Guide Thinking and Analysis Regarding Climate Change Policies." *Risk Analysis* 21(6): 989–1000. 2001.
- Keeney, Ralph L., and Howard Raiffa. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Cambridge, UK: Cambridge University Press, 1993.
- Kirwin, B., and L. K. Ainsworth. *A Guide to Task Analysis*. London: Taylor and Francis, 1992.
- Kurke, M. I. "Operational Sequence Diagrams in System Design." *Human Factors* 3: 66–73. 1961.
- Long, Jim. *Relationships Between Common Graphical Representations in Systems Engineering*. Vienna, VA: Vitech Corporation, 2002.
- Martin, James N. *Processes for Engineering a System: An Overview of the ANSI/GEIA EIA-632 Standard and Its Heritage*. New York: Wiley & Sons, 2000.
- . *Systems Engineering Guidebook: A Process for Developing Systems and Products*. Boca Raton: CRC Press, 1996.
- Meister, David. *Behavioral Analysis and Measurement Methods*. New York: John Wiley & Sons, 1985.
- . *Human Factors: Theory and Practice*. New York: John Wiley & Sons, 1971.
- Miao, Y., and J. M. Haake. "Supporting Concurrent Design by Integrating Information Sharing and Activity Synchronization." In *Proceedings of the 5th ISPE International Conference on Concurrent Engineering Research and Applications (CE98)*. Tokyo, 1998, pp. 165–74.
- The Mitre Corporation. *Common Risks and Risk Mitigation Actions for a COTS-based System*. McLean, VA.
- Morgan, M. Granger, and M. Henrion. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge, UK: Cambridge University Press, 1990.
- NASA. *Final Memorandum on NASA's Acquisition Approach Regarding Requirements for Certain Software Engineering Tools to Support NASA Programs*, Assignment No. S06012. Washington, DC, NASA Office of Inspector General, 2006.
- . *NASA Cost Estimating Handbook*. Washington, DC, 2004.
- . *NASA-STD-3001, NASA Space Flight Human System Standard Volume 1: Crew Health*. Washington, DC, 2007.
- . *NASA-STD-(I)-7009, Standard for Models and Simulations*. Washington, DC, 2006.
- . *NASA-STD-8719.13, Software Safety Standard, NASA Technical Standard, Rev B*. Washington, DC, 2004.
- . *NASA-STD-8729.1, Planning, Developing, and Maintaining and Effective Reliability and Maintainability (R&M) Program*. Washington, DC, 1998.
- . *NOAA N-Prime Mishap Investigation Final Report*. Washington, DC, 2004.
- . *NPD 2820.1, NASA Software Policy*. Washington, DC, 2005.
- . *NPD 8010.2, Use of the SI (Metric) System of Measurement in NASA Programs*. Washington, DC, 2007.
- . *NPD 8010.3, Notification of Intent to Decommission or Terminate Operating Space Systems and Terminate Missions*. Washington, DC, 2004.
- . *NPD 8020.7, Biological Contamination Control for Outbound and Inbound Planetary Spacecraft*. Washington, DC, 1999.
- . *NPD 8070.6, Technical Standards*. Washington, DC, 2003.
- . *NPD 8730.5, NASA Quality Assurance Program Policy*. Washington, DC, 2005.

- . *NPR 1441.1, NASA Records Retention Schedules*. Washington, DC, 2003.
- . *NPR 1600.1, NASA Security Program Procedural Requirements*. Washington, DC, 2004.
- . *NPR 2810.1, Security of Information Technology*. Washington, DC, 2006.
- . *NPR 7120.5, NASA Space Flight Program and Project Management Processes and Requirements*. Washington, DC, 2007.
- . *NPR 7120.6, Lessons Learned Process*. Washington, DC, 2007.
- . *NPR 7123.1, Systems Engineering Processes and Requirements*. Washington, DC, 2007.
- . *NPR 7150.2, NASA Software Engineering Requirements*. Washington, DC, 2004.
- . *NPR 8000.4, Risk Management Procedural Requirements*. Washington, DC, NASA Office of Safety and Mission Assurance, 2007.
- . *NPR 8020.12, Planetary Protection Provisions for Robotic Extraterrestrial Missions*. Washington, DC, 2004.
- . *NPR 8580.1, Implementing The National Environmental Policy Act and Executive Order 12114*. Washington, DC, 2001.
- . *NPR 8705.2, Human-Rating Requirements for Space Systems*. Washington, DC, 2005.
- . *NPR 8705.3, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Washington, DC, 2002.
- . *NPR 8705.4, Risk Classification for NASA Payloads*. Washington, DC, 2004.
- . *NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects*. Washington, DC, 2004.
- . *NPR 8710.1, Emergency Preparedness Program*. Washington, DC, 2006.
- . *NPR 8715.2, NASA Emergency Preparedness Plan Procedural Requirements—Revalidated*. Washington, DC, 1999.
- . *NPR 8715.3, NASA General Safety Program Requirements*. Washington, DC, 2007.
- . *NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris*. Washington, DC, 2007.
- . *NPR 8735.2, Management of Government Quality Assurance Functions for NASA Contracts*. Washington, DC, 2006.
- . *NSS-1740.14, NASA Safety Standard Guidelines and Assessment Procedures for Limiting Orbital Debris*. Washington, DC, 1995.
- . *Off-the-Shelf Hardware Utilization in Flight Hardware Development*, MSFC NASA MWI 8060.1 Rev A. Washington, DC, 2004.
- . *Off-the-Shelf Hardware Utilization in Flight Hardware Development*, JSC Work Instruction EA-WI-016. Washington, DC.
- . *Project Management: Systems Engineering & Project Control Processes and Requirements*, JPR 7120.3. Washington, DC, 2004.
- . *The SEB Source Evaluation Process*. Washington, DC, 2001.
- . *Solicitation to Contract Award*. Washington, DC, NASA Procurement Library, 2007.
- . *Statement of Work Checklist*. Washington, DC.
- . *System and Software Metrics for Performance-Based Contracting*. Washington, DC.
- . *Systems Engineering Handbook*, SP-6105. Washington, DC, 1995.
- . *Training Manual for Elements of Interface Definition and Control*, NASA Reference Publication 1370. Washington, DC, 1997.

- NASA Langley Research Center. *Instructional Handbook for Formal Inspections*.
- . *Guidance on System and Software Metrics for Performance-Based Contracting*. National Defense Industrial Association. *Data Management*, ANSI/GEIA GEIA-859. Arlington, VA, 2004.
- . *National Consensus Standard for Configuration Management*, ANSI/GEIA EIA-649, Arlington, VA, 1998.
- Naval Air Systems Command. *Systems Command SE Guide: 2003* (based on requirements of ANSI/EIA 632: 1998). Patuxent River, MD, 2003.
- Nuclear Regulatory Commission. *NUREG-0700, Human-System Interface Design Review Guidelines, Rev. 2*. Washington, DC, Office of Nuclear Regulatory Research, 2002.
- . *Systems Engineering Guide*. Patuxent River, MD, 2003.
- Price, H. E. “The Allocation of Functions in Systems.” *Human Factors* 27: 33–45. 1985.
- The Project Management Institute®. *Practice Standards for Work Breakdown Structures*. Newtown Square, PA, 2001.
- Rechtin, Eberhardt. *Systems Architecting of Organizations: Why Eagles Can't Swim*. Boca Raton: CRC Press, 2000.
- Saaty, Thomas L. *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980.
- Sage, Andrew, and William Rouse. *The Handbook of Systems Engineering and Management*. New York: Wiley & Sons, 1999.
- Shafer, J. B. “Practical Workload Assessment in the Development Process.” In *Proceedings of the Human Factors Society 31st Annual Meeting*. Santa Monica: Human Factors Society, 1987.
- Stamelatos, M., H. Dezfuli, and G. Apostolakis. “A Proposed Risk-Informed Decisionmaking Framework for NASA.” In *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*. New Orleans, LA, May 14–18, 2006.
- Stern, Paul C., and Harvey V. Fineberg, eds. *Understanding Risk: Informing Decisions in a Democratic Society*. Washington, DC: National Academies Press, 1996.
- Taylor, Barry. *Guide for the Use of the International System of Units (SI)*, Special Publication 811. Gaithersburg, MD: National Institute of Standards and Technology, Physics Laboratory, 2007.
- U.S. Air Force. *SMC Systems Engineering Primer and Handbook*, 3rd ed. Los Angeles: Space & Missile Systems Center, 2005.
- U.S. Army Research Laboratory. *Design Guidance for Producibility*, MIL HDBK 727. Adelphi, MD: Weapons and Materials Research Directorate, 1990.
- . White Paper on Risk-Informed and Performance-Based Regulation, SECY-98-144. Washington, DC, 1998.

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传 真：（010）88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

○ 内容简介

系统工程是分析解决复杂系统的论证、设计、生产和使用中的评价决策和权衡优化问题的有效方法和手段。系统工程不仅有完整的理论方法和技术手段构成的科学体系，而且在像航天系统这样经费预算多、研制周期长、运行使用风险高的复杂系统中的具体应用又体现出多样性和复杂性。如何有效地利用系统工程理论和方法针对复杂系统进行组织管理并达到预期的目的，需要对系统工程思想有深刻的理解和丰富的工程实践经验。本手册是美国国家航空航天局（NASA）对多年系统工程实践经验的总结，主要有三个部分的内容：第一部分（第1~3章）是结合航天产品的寿命周期介绍由多个系统工程流程构成的航天产品开发和控制管理的系统工程引擎，第二部分（第4~5章）针对系统工程引擎中的每个流程详细介绍流程实施的过程和指南，第三部分（第6~7章）介绍在开展系统工程工作时应当把握的关键技术和相关标准。

本手册内容翔实、图文并茂，许多问题的阐述结合实例，部分具体操作还在附录中给出了参考样板。NASA系统工程手册不仅可以作为工业工程领域产品开发和系统工程组织管理实践的有益借鉴，也可以作为从事产品研发与项目管理的科技人员和高等院校系统工程专业或相近专业研究生和高年级本科生的学习参考。



责任编辑：陈韦凯

封面设计：一克米工作室



ISBN 978-7-121-18081-1



9 787121 180811 >

定价：65.00元